29[E] CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29[TH] INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Atelier
Dragon : *La sécurité publique*
Le crime sur Internet

Workshop
“Public Safety” Dragon
Internet Crime

28 septembre/Septembre 28
9h – 11h15

Série Terra Incognita, cahier de travail # 17/Terra Incognita, workbook series # 17



Table des matières / Table of contents

Biographies

Président : M. Wayne Watson

Wayne Watson est directeur général de la Direction des enquêtes et des demandes de renseignements du Commissariat à la protection de la vie privée du Canada (CPVP). Il est officier commissionné à la retraite de la Gendarmerie royale du Canada (GRC) où il a été en poste pendant 31 ans à Montréal, à Valleyfield, à Québec et dans la région de la capitale nationale. Avant de se joindre au CPVP en août 2006, le surintendant principal Watson était chef du Service divisionnaire des infractions commerciales de la GRC, à Ottawa. M. Watson a étudié le droit et l'administration à l'Université Laval, dans sa ville natale, Québec. Il a également rédigé des articles sur des sujets variés, notamment le leadership, la corruption et l'éthique pour diverses publications dans le domaine de l'application de la loi.

Conférenciers

Mme Deborah Platt Majoras, Ph. D.

Deborah Platt Majoras est l'actuelle présidente de la Commission fédérale du commerce (CFC) des États-Unis. Avant sa nomination, Mme Majoras a travaillé en qualité de partenaire à la section antitrust du cabinet d'avocat Jones Day à Washington D.C. et a également fait partie du département chargé des questions liées à la technologie. Elle avait auparavant exercé les fonctions de sous-procureure générale adjointe de la division antitrust au département de la Justice des États-Unis. Au cours de son mandat, elle a été présidente du groupe de travail sur les fusions du Réseau international de la concurrence (RIC) et a coordonné diverses initiatives stratégiques comme les audiences de la CFC et du département de la Justice sur les services de santé, l'initiative du département de la Justice concernant le processus d'examen des fusions et le projet sur les pratiques exemplaires en matière de fusions. Mme Majoras est titulaire d'un baccalauréat du collège Westminster et d'un doctorat en droit de l'Université de Virginie. Elle est membre de la section du droit antitrust de l'American Bar Association, où elle a exercé les fonctions de vice-présidente du Comité concernant l'article 2 et a fait partie du Comité de planification à long terme. En outre,

Biographies

Chair : Mr. Wayne Watson

Wayne Watson is the Director General of the Investigations and Inquiries Branch of the Office of the Privacy Commissioner of Canada (OPC). He is a retired commissioned officer of the Royal Canadian Mounted Police (RCMP) where he served for thirty–one years in Montreal, Valleyfield, Quebec City and the National Capital Region. Prior to joining the OPC in August 2006, (Chief Superintendent) Mr. Watson was Head of the RCMP Commercial Crime Branch in Ottawa. Wayne Watson studied Law and Administration at Laval University in his hometown of Quebec City. He has also penned articles on various topics including leadership, and corruption and ethics for different law enforcement publications.

Speakers

Dr. Deborah Platt Majoras

Deborah Platt Majoras is current Chairman of the U.S. Federal Trade Commission. Prior to her appointment, Majoras served as a partner in the antitrust section at Jones Day in Washington, DC, and also as a member of the firm's technology issues practice. She previously served as deputy assistant attorney general and principal deputy at the U.S. Department of Justice's (DOJ) Antitrust Division. During her tenure, she served as chair of the International Competition Network's (ICN) Merger Working Group and oversaw policy initiatives such as the FTC/DOJ Health Care Hearings, DOJ's Merger Review Process Initiative, and the Mergers Best Practices Project. Majoras holds a BA from Westminster College and a J.D. from the University of Virginia. She is a member of the American Bar Association's Section of Antitrust Law, where she served as vice chair of the Section 2 Committee and as a member of the Long-Range Planning Committee. Majoras also served as a non-governmental advisor to the ICN and was named by President Bush to serve on the Antitrust Modernization Commission.

Deborah Platt Majoras a travaillé en qualité de conseillère non gouvernementale au RIC et a été nommée par le président Bush pour siéger à l'Antitrust Modernization Commission (commission sur la modernisation des lois antitrust).

Mme Cynthia Fraser

Cynthia Fraser est spécialiste de la sécurité de la technologie pour le Safety Net: Safe & Strategic Technology Project (projet de technologies stratégiques et sécuritaires « Safety Net ») du US National Network to End Domestic Violence (réseau national des États-Unis pour l'élimination de la violence familiale). Mme Fraser offre une formation et une assistance technique internationales en ce qui a trait aux répercussions de la technologie sur les anciennes victimes de harcèlement criminel et de violence familiale et sexuelle. Pendant ses 18 années de travail dans les systèmes canadiens et américains, Mme Fraser a doté en personnel des services d'assistance téléphonique et des refuges, a accompagné des victimes par le biais des services judiciaires et des services sociaux et a formé des groupes multidisciplinaires Elle a également travaillé pour le compte de divers organismes nationaux de politiques et de recherches comme le US Institute for Women's Policy Research (institut de recherches des États-Unis sur les politiques relatives aux femmes) et le National Resource Center on Domestic Violence (centre national de ressources sur la violence familiale). Elle a fait partie de comités consultatifs nationaux et elle est coauteure de plusieurs publications. Elle est en outre titulaire de diplômes en sciences politiques et en psychologie. Mme Fraser utilise son expérience des technologies d'assistance et des technologies liées à la surveillance, à l'information et aux communications pour renforcer les capacités et promouvoir des politiques et des pratiques qui accordent la priorité à la sécurité et à l'accessibilité, et au respect du droit à la vie privée de toutes les victimes de violence.

Ms. Cynthia Fraser

Cynthia Fraser is a Technology Safety Specialist for Safety Net: Safe & Strategic Technology Project of the US National Network to End Domestic Violence. Ms. Fraser provides international training and technical assistance on addressing technology's impact on survivors of stalking, domestic and sexual violence. During 18 years working in Canadian and American systems, Ms. Fraser has staffed hotlines and shelters, accompanied survivors through court and social services, trained multidisciplinary groups, and worked in such national policy and research organisations as the US Institute for Women's Policy Research and the National Resource Center on Domestic Violence. She has sat on national advisory committees, coauthored several publications, and holds degrees in Political Science and Psychology. Ms. Fraser uses her experience with surveillance, information, communication and assistive technologies to build capacity and promote policy and practice that prioritizes the safety, accessibility, and privacy rights for all survivors of violence.

M. Dean Turner

Dean Turner est le directeur du Réseau d'information mondial de Symantec Corporation, où il travaille en étroite collaboration avec l'équipe de recherche avancée sur les menaces en vue de déterminer quelles formes prendront les menaces liées à Internet. M. Turner s'occupe aussi de la

Mr. Dean Turner

Dean Turner is the Director of Symantec Corp.'s Global Intelligence Network (GIN) where he works closely with Symantec's Advanced Threat Research team to identify shifts in the Internet threat landscape. Mr. Turner also manages Symantec's security intelligence and data feeds

gestion du renseignement de sécurité et de la stratégie d'incorporation des données de Symantec, et il est le directeur de la rédaction du très remarqué *Internet Security Threat Report* (rapport sur la menace à la sécurité dans Internet) de Symantec, un rapport détaillé qui paraît deux fois l'an. Avant de se joindre à Symantec, il a cofondé SecurityFocus, où il était le directeur des opérations et du contenu jusqu'à ce que la compagnie soit acquise par Symantec en 2002. M. Turner est titulaire d'un baccalauréat en science politique et en études stratégiques de l'Université de Calgary (Canada) et d'une maîtrise en stratégie sur la sécurité de l'Université de Hull (Royaume-Uni). Il se prépare actuellement à présenter sa thèse pour obtenir un doctorat en cyberguerre et en infodominance.

strategy and is Executive Editor of Symantec's highly successful Internet Security Threat Report (ISTR), a twice-yearly report detailing the Internet threat landscape. Before joining Symantec, he was a co-founder of SecurityFocus, serving as Director of Operations and Content until the company's acquisition by Symantec in 2002. Dean Turner has a BA in political science and strategic studies from the University of Calgary, Canada, and a Master's degree in security strategy from the University of Hull, U.K. He is currently working on a thesis submission for his doctorate in information warfare and dominance.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Lutte contre le vol d'identité
Plan stratégique

Combating Identity Theft
A Strategic Plan

Commission fédérale du commerce

Federal Trade Commission



Résumé

De la rue principale à Wall Street, de la véranda arrière au bureau de direction, de la table de cuisine à la table de conférence, les Américains parlent de vol d'identité. La raison en est simple : chaque année, des millions d'Américains subissent des traumatismes émotionnels découlant de pertes financières. Ce crime prend diverses formes mais laisse invariablement aux victimes la tâche de réparer les pots cassés. Il s'agit d'un problème qui n'a pas de cause ni de solution unique.

A. INTRODUCTION

Il y a huit ans, le Congrès adoptait l'Identity Theft and Assumption Deterrence Act[1], une loi faisant du vol d'identité un crime fédéral, et confiait à la Commission fédérale du commerce (CFC) la responsabilité de recevoir les plaintes des victimes de vol d'identité, de les communiquer à la police fédérale, étatique et locale, et de fournir aux victimes les renseignements nécessaires pour qu'elles puissent rétablir leur réputation. Depuis lors, des organismes fédéraux, étatique et locaux ont pris des mesures vigoureuses pour lutter contre le vol d'identité. La CFC a mis sur pied un bureau central de données sur le vol d'identité, une ressource essentielle pour les consommateurs et les organismes d'exécution de la loi; le département de la Justice (DJ) a vigoureusement poursuivi les responsables d'une vaste gamme de stratagèmes de vol d'identité en vertu de lois applicables au vol d'identité et d'autres lois; les organismes fédéraux de réglementation financière[2] ont adopté et appliqué de solides normes de sécurité des données pour les entités qui relèvent de leur compétence; le Congrès a adopté la REAL ID Act de 2005 et le département de la Sécurité intérieure a pris un règlement provisoire en vertu de cette loi; et plusieurs autres organismes fédéraux comme l'administration américaine de la Sécurité sociale (Social Security Administration) ont cherché à renseigner les consommateurs sur la façon d'éviter le vol d'identité et de rétablir leur identité. Bon nombre d'entités du secteur privé ont également pris des mesures proactives et importantes afin de protéger les données contre les vols d'identité, de renseigner les consommateurs sur la façon d'éviter le vol d'identité, d'aider la police à appréhender les voleurs d'identité et d'aider les victimes qui

Executive Summary

From Main Street to Wall Street, from the back porch to the front office, from the kitchen table to the conference room, Americans are talking about identity theft. The reason: millions of Americans each year suffer the financial and emotional trauma it causes. This crime takes many forms, but it invariably leaves victims with the task of re-pairing the damage to their lives. It is a prob-lem with no single cause and no single solution.

A. INTRODUCTION

Eight years ago, Congress enacted the Identity Theft and Assumption Deterrence Act, which created the federal crime of identity theft and charged the Federal Trade Commission (FTC) with taking complaints from identity theft victims, sharing these complaints with federal, state, and local law enforcement, and providing the victims with information to help them restore their good name. Since then, federal, state, and local agencies have taken strong action to combat identity theft. The FTC has developed the Identity Theft Data Clearinghouse into a vital resource for consumers and law enforcement agencies; the Department of Justice (DOJ) has prosecuted vigorously a wide range of identity theft schemes under the identity theft statutes and other laws; the federal financial regulatory agencies have adopted and enforced robust data security standards for entities under their jurisdiction; Congress passed, and the Department of Homeland Security issued draft regulations on, the REAL ID Act of 2005; and numerous other federal agencies, such as the Social Security Administration (SSA), have educated consumers on avoiding and recovering from identity theft. Many private sector entities, too, have taken proactive and significant steps to protect data from identity thieves, educate consumers about how to prevent identity theft, assist law enforcement in apprehending identity thieves, and assist identity theft victims who suffer losses.

Over those same eight years, however, the problem of identity theft has become more complex and challenging for the general public, the government, and the private sector. Consumers, overwhelmed with weekly media reports of data breaches, feel vulnerable and uncertain of how to protect their identities. At the same time, both the private and public sectors have had to grapple with difficult, and costly, decisions about invest-

subissent des pertes.

Au cours de ces huit années, le problème du vol d'identité est devenu plus complexe et plus intimidant pour le grand public, le gouvernement et le secteur privé. Les consommateurs, dépassés par les rapports hebdomadaires des médias concernant des brèches dans la protection de données, se sentent vulnérables et sont incertains quant à la façon de protéger leur identité. De même, les secteurs privé et public ont dû prendre des décisions difficiles et faire des investissements coûteux pour établir des garanties et pour tenter de mieux protéger le public. Le vol d'identité nécessite de plus en plus d'interventions de la part des autorités policières à tous les niveaux de gouvernement, qu'il s'agisse des plus grandes villes ayant d'importants services de police ou des plus petites villes ayant un seul détective affecté aux fraudes.

Les observations publiques ont aidé le Groupe de travail à définir les questions et les enjeux que pose le vol d'identité et à formuler des réponses stratégiques. Pour s'assurer d'obtenir le point de vue de tous les intervenants, le Groupe de travail a sollicité l'apport du public.

En plus des groupes de défense des intérêts des consommateurs, de la police, du milieu des affaires et de l'industrie, le Groupe de travail a aussi reçu des commentaires de la part de victimes de vol d'identité3. Ces dernières ont fait état du fardeau et des frustrations associées au rétablissement à la suite de ce crime. Les cas rapportés mettent l'accent sur la nécessité pour le gouvernement d'agir rapidement pour aborder ce problème.

L'immense majorité des commentaires reçus par le Groupe de travail mettent clairement en lumière la nécessité d'une approche entièrement coordonnée à la lutte contre le vol d'identité grâce à la prévention, à la sensibilisation, à l'exécution de la loi, à la formation et à l'aide aux victimes. Les consommateurs qui ont écrit au Groupe de travail prient celui-ci d'exhorter les secteurs public et privé à mieux protéger les numéros d'assurance sociale (NAS), et plusieurs des personnes qui ont fait des commentaires ont abordé les défis que pose la sur-utilisation de ce numéro comme moyen d'identification. D'autres commentaires venant de certains secteurs des affaires font état des usages utiles du NAS pour la détection des fraudes. Le Groupe de travail a pris

ments in safeguards and what more to do to protect the public. And, at every level of government—from the largest cities with major police departments to the smallest towns with one fraud detective—identity theft has placed increasingly pressing demands on law enforcement.

Public comments helped the Task Force define the issues and challenges posed by identity theft and develop its strategic responses. To ensure that the Task Force heard from all stakeholders, it solicited comments from the public.

In addition to consumer advocacy groups, law enforcement, business, and industry, the Task Force also received comments from identity theft victims themselves. The victims wrote of the burdens and frustrations associated with their recovery from this crime. Their stories reaffirmed the need for the government to act quickly to address this problem.

The overwhelming majority of the comments received by the Task Force strongly affirmed the need for a fully coordinated approach to fighting the problem through prevention, awareness, enforcement, training, and victim assistance. Consumers wrote to the Task Force exhorting the public and private sectors to do a better job of protecting their Social Security numbers (SSNs), and many of those who submitted comments discussed the challenges raised by the overuse of Social Security numbers as identifiers. Others, representing certain business sectors, pointed to the beneficial uses of SSNs in fraud detection. The Task Force was mindful of both considerations, and its recommendations seek to strike the appropriate balance in addressing SSN use. Local law enforcement officers, regardless of where they work, wrote of the challenges of multi-jurisdictional investigations, and called for greater coordination and resources to support the investigation and prosecution of identity thieves. Various business groups described the steps they have taken to minimize the occurrence and impact of the crime, and many expressed support for risk-based, national data security and breach notification requirements.

These communications from the public went a long way toward informing the Task Force's recommendation for a fully coordinated strategy. Only an approach that encompasses effective prevention, public awareness and edu-cation, victim assistance, and law enforcement measures, and

bonne note des deux points de vue et ses recommandations visent à trouver un bon équilibre dans l'utilisation du NAS. Les responsables locaux de l'exécution de la loi, sans égard à leur lieu de travail, ont fait état des défis que posent les enquêtes qui couvrent plusieurs secteurs de compétences et ont réclamé davantage de coordination et de ressources pour appuyer les enquêtes et pour poursuivre les voleurs d'identité devant les tribunaux. Divers groupes d'affaires ont décrit les mesures prises pour minimiser l'occurrence et les répercussions de ce crime, et bon nombre ont exprimé leur appui en faveur de mesures de sécurité nationale des données basées sur le risque et sur les exigences en matière de notification en cas de brèches dans la protection des données.

Ces documents fournis par le public ont beaucoup contribué à la formulation des recommandations du Groupe de travail en vue d'une pleine coordination. Seule une approche englobant la prévention efficace, la sensibilisation et l'éducation du public, l'aide aux victimes et des mesures d'application de la loi, et qui engage entièrement les autorités fédérales, étatiques et locales permettra de protéger les citoyens et les entités privées contre le crime.

B. LA STRATÉGIE

Bien que le vol d'identité soit défini de plusieurs façons, il s'agit essentiellement d'une utilisation abusive des renseignements personnels d'une personne pour commettre une fraude. Il y a au moins trois stades au cycle de vie du vol d'identité, et chacun doit être abordé.

Premièrement, le vol d'identité consiste à se procurer les renseignements personnels d'une victime.

Les criminels doivent d'abord se procurer les renseignements personnels, soit par des moyens peu compliqués – comme le vol de courrier ou de dossiers sur les lieux de travail ou la « collecte » dans les bacs à ordures – soit par des moyens plus complexes et des fraudes de haute technologie comme le piratage et l'utilisation de codes machine malveillants. En soi, la perte ou le vol de renseignements personnels n'entraîne pas immédiatement le vol d'identité. Dans certains cas, ceux qui volent des articles personnels volent aussi par inadvertance des renseignements

fully engages federal, state, and local authorities will be successful in protecting citizens and private entities from the crime.

B. THE STRATEGY

Although identity theft is defined in many different ways, it is, fundamentally, the misuse of another individual's personal information to commit fraud. Identity theft has at least three stages in its "life cycle," and it must be attacked at each of those stages:

First, the identity thief attempts to acquire a victim's personal information.

Criminals must first gather personal information, either through low-tech methods—such as stealing mail or workplace records, or "dumpster diving" —or through complex and high-tech frauds, such as hacking and the use of malicious computer codes. The loss or theft of personal information by itself, however, does not immediately lead to identity theft. In some cases, thieves who steal personal items inadvertently steal personal information that is stored in or with the stolen personal items, yet never make use of the personal information. It has recently been reported that, during the past year, the personal records of nearly 73 million people have been lost or stolen, but that there is no evidence of a surge in identity theft or financial fraud as a result. Still, because any loss or theft of personal information is troubling and potentially devastating for the persons involved, a strategy to keep consumer data out of the hands of criminals is essential.

Second, the thief attempts to misuse the information he has acquired.

In this stage, criminals have acquired the victim's personal information and now attempt to sell the information or use it themselves. The misuse of stolen personal information can be classified in the following broad categories:

► **Existing account fraud:** This occurs when thieves obtain account information involving credit, brokerage, banking, or utility accounts that are already open. Existing account fraud is typically a less costly, but more prevalent, form of identity theft. For example, a stolen credit card may lead to thousands of dollars in fraudulent charges, but the card generally

personnels qui sont contenus dans les articles volés ou qui sont conservés avec ces articles et ne font jamais usage des renseignements personnels. Récemment, on a rapporté qu'au cours de l'année écoulée, les dossiers personnels de près de 73 millions de personnes avaient été perdus ou volés sans qu'il n'y ait preuve d'un accroissement du nombre de vols d'identité ou de fraudes financières découlant de ces vols ou de ces pertes. Tout de même, puisque le vol et la perte de renseignements personnels sont sources de préoccupations et peuvent avoir des conséquences potentiellement dévastatrices pour les personnes touchées, il est essentiel d'en arriver à une stratégie pour éviter que les données des consommateurs ne tombent entre les mains de criminels.

Deuxièmement, le voleur tente d'utiliser à mauvais escient les renseignements acquis.

À ce stade, les criminels se sont procurés les renseignements personnels d'une victime et tentent de vendre ces renseignements ou de les utiliser eux-mêmes. L'utilisation abusive de renseignements personnels volés peut faire partie de l'une ou l'autre des grandes catégories suivantes :

- ► **Fraude avec un compte existant :** Cela se produit lorsque les voleurs obtiennent des renseignements sur les comptes de crédit, de courtage, de banque ou de services publics déjà existants. La fraude concernant les comptes existants est une forme de vol d'identité généralement moins coûteuse mais plus courante. Par exemple, une carte de crédit volée peut mener à des achats frauduleux totalisant des milliers de dollars mais la carte ne fournit habituellement pas suffisamment de renseignements au voleur pour établir une fausse identité. De plus, la plupart des émetteurs de cartes de crédit ont pour politique de ne pas tenir les consommateurs responsables des débits frauduleux, et la législation fédérale limite à 50 $ la responsabilité des victimes de vol de cartes de crédit.

- ► **Fraude avec un nouveau compte :** Les voleurs utilisent des renseignements personnels comme le numéro d'assurance sociale, la date de naissance et l'adresse domiciliaire pour ouvrir de nouveaux comptes au nom de la victime et faire des achats sans

would not provide the thief with enough information to establish a false identity. Moreover, most credit card companies, as a matter of policy, do not hold consumers liable for fraudulent charges, and federal law caps liability of victims of credit card theft at $50.

- ► **New account fraud:** Thieves use personal information, such as Social Security numbers, birth dates, and home addresses, to open new accounts in the victim's name, make charges indiscriminately, and then disappear. While this type of identity theft is less likely to occur, it imposes much greater costs and hardships on victims.

In addition, identity thieves sometimes use stolen personal information to obtain government, medical, or other benefits to which the criminal is not entitled.

Third, an identity thief has completed his crime and is enjoying the benefits, while the victim is realizing the harm.

At this point in the life cycle of the theft, victims are first learning of the crime, often after being denied credit or employment, or being contacted by a debt collector seeking payment for a debt the victim did not incur.

In light of the complexity of the problem at each of the stages of this life cycle, the Identity Theft Task Force is recommending a plan that marshals government resources to crack down on the criminals who traffic in stolen identities, strengthens efforts to protect the personal information of our nation's citizens, helps law enforcement officials investigate and prosecute identity thieves, helps educate consumers and businesses about protecting themselves, and increases the safeguards on personal data entrusted to federal agencies and private entities.

The Plan focuses on improvements in four key areas:

- ► keeping sensitive consumer data out of the hands of identity thieves through better data security and more accessible education;

- ► making it more difficult for identity thieves who obtain consumer data to use it to steal identities;

discernement avant de disparaître. Bien que ce type de vol d'identité soit moins fréquent, il entraîne des coûts beaucoup plus importants et des difficultés bien plus grandes pour les victimes.

En outre, les voleurs d'identité se servent parfois de renseignements personnels volés pour obtenir des services gouvernementaux, médicaux ou d'autres avantages auxquels ils n'ont pas droit.

Troisièmement, le voleur d'identité a commis son crime et profite des retombées, tandis que la victime en subit les conséquences.

À ce stade du cycle de vie du vol d'identité, la victime découvre le crime qui a été commis, bien souvent après avoir essuyé un refus de crédit ou d'emploi ou après avoir été contactée par une agence de recouvrement cherchant à obtenir le remboursement d'une dette que la victime n'a pas contractée.

Compte tenu de la complexité du problème à chaque étape de ce cycle de vie, le Groupe de travail sur le vol d'identité recommande un plan d'action qui mobilise les ressources du gouvernement en vue de sévir contre les criminels qui font le trafic d'identités volées, d'accroître les efforts de protection des renseignements personnels des citoyens du pays, d'aider les responsables de l'application de la loi à enquêter sur les vols et à poursuivre les voleurs d'identité, d'aider à éduquer les consommateurs et les entreprises sur la façon de se protéger, et d'augmenter les garanties concernant les données personnelles confiées à des organismes fédéraux et à des entités privées.

Le plan vise à apporter des améliorations dans quatre secteurs clés :

► éviter que les données sensibles sur les consommateurs ne tombent entre les mains de voleurs d'identité grâce à de meilleures mesures de protection des données et à une éducation plus accessible;

► faire en sorte qu'il soit plus difficile pour les voleurs d'identité d'utiliser les données sur les consommateurs pour usurper des identités;

► aider les victimes de vol d'identité à se remettre des conséquences du crime;

► assisting the victims of identity theft in recovering from the crime; and

► deterring identity theft by more aggressive prosecution and punishment of those who commit the crime.

In these four areas, the Task Force makes a number of recommendations summarized in greater detail below. Among those recommendations are the following broad policy changes:

► that federal agencies should reduce the unnecessary use of Social Security numbers (SSNs), the most valuable commodity for an identity thief;

► that national standards should be established to require private sector entities to safeguard the personal data they compile and maintain and to provide notice to consumers when a breach occurs that poses a significant risk of identity theft;

► that federal agencies should implement a broad, sustained awareness campaign to educate consumers, the private sector, and the public sector on deterring, detecting, and defending against identity theft; and

► that a National Identity Theft Law Enforcement Center should be created to allow law enforcement agencies to coordinate their efforts and information more efficiently, and investigate and prosecute identity thieves more effectively.

The Task Force believes that all of the recommendations in this strategic plan—from these broad policy changes to the small steps—are necessary to wage a more effective fight against identity theft and reduce its incidence and damage. Some recommendations can be implemented relatively quickly; others will take time and the sustained cooperation of government entities and the private sector. Following are the recommendations of the President's Task Force on Identity Theft:

PREVENTION: KEEPING CONSUMER DATA OUT OF THE HANDS CRIMINALS

Identity theft depends on access to consumer data. Reducing the opportuni-ties for thieves to get the data is critical to fighting the crime. Gov-

- ► décourager le vol d’identité en poursuivant avec détermination les voleurs d’identité et en leur imposant des peines plus lourdes.

Le Groupe de travail a formulé certaines recommandations concernant ces quatre situations. Elles sont reprises plus loin de manière plus détaillée. Les grands changements de politique suivants font partie de ces recommandations :

- ► que les organismes fédéraux réduisent les utilisations inutiles du numéro d’assurance sociale (NAS), l’élément le plus utile pour un voleur d’identité;

- ► que l’on adopte des normes nationales pour exiger que les entités du secteur privé protègent les données personnelles qu’elles recueillent et conservent et qu’elles soient tenues d’aviser les consommateurs en cas de brèches posant un risque important de vol d’identité;

- ► que les organismes fédéraux mettent en œuvre une vaste campagne soutenue pour informer les consommateurs, le secteur privé et le secteur public de la façon de contrer et de détecter le vol d’identité et de se protéger contre ce type de vol;

- ► qu’un centre national d’application de la loi concernant le vol d’identité soit créé pour que les organismes d’exécution de la loi coordonnent leurs efforts et leurs renseignements de manière plus efficace, enquêtent mieux sur les vols d’identité et poursuivent plus efficacement les voleurs.

Le Groupe de travail estime que toutes les recommandations de ce plan stratégique – depuis les grands changements de politique jusqu’aux petites étapes – sont nécessaires pour mieux lutter contre le vol d’identité et pour en réduire l’incidence et les conséquences. Certaines recommandations peuvent être mises en œuvre assez rapidement, tandis que d’autres exigeront du temps et une coordination soutenue de la part des entités gouvernementales et du secteur privé. Voici les recommandations du Groupe de travail du Président sur le vol d’identité.

ernment, the business community, and consumers have roles to play in protecting data.

Data compromises can expose consumers to the threat of identity theft or related fraud, damage the reputation of the entity that experienced the breach, and carry financial costs for everyone involved. While “perfect security” does not exist, all entities that collect and maintain sensitive consumer information must take reasonable and appropriate steps to protect it.

Data Security in Public Sector

- ► Decrease the Unnecessary Use of Social Security Numbers in the Public Sector by Developing Alternative Strategies for Identity Management
  - Survey current use of SSNs by federal government
  - Issue guidance on appropriate use of SSNs
  - Establish clearinghouse for “best” agency practices that minimize use of SSNs
  - Work with state and local governments to review use of SSNs

- ► Educate Federal Agencies on How to Protect Data; Monitor Their Compliance with Existing Guidance
  - Develop concrete guidance and best practices
  - Monitor agency compliance with data security guidance
  - Protect portable storage and communications devices

- ► Ensure Effective, Risk-Based Responses to Data Breaches Suffered by Federal Agencies
  - Issue data breach guidance to agencies
  - Publish a “routine use” allowing disclosure of information after a breach to those entities that can assist in responding to the breach

Data Security in Private Sector

- ► Establish National Standards for Private Sector Data Protection Requirements and Breach Notice Requirements

- ► Develop Comprehensive Record on Private Sector Use of Social Security Numbers

- ► Better Educate the Private Sector on Safe-

PRÉVENTION : ÉVITER QUE LES DONNÉES SUR LES CONSOMMATEURS NE TOMBENT ENTRE LES MAINS DE CRIMINELS

Le vol d'identité est lié à l'accès aux données sur les consommateurs. Pour contrer ce crime, il importe de réduire les occasions pour les voleurs de s'approcher des données. Le gouvernement, le milieu des affaires et les consommateurs ont un rôle à jouer dans la protection des données.

Les brèches dans la protection des données peuvent rendre les consommateurs vulnérables au vol d'identité ou à des fraudes connexes, nuire à la réputation de l'entité victime de la brèche, et avoir des conséquences financières pour toutes les parties en cause. Bien que la « sécurité parfaite » n'existe pas, toutes les entités qui recueillent et conservent des données sensibles sur les consommateurs doivent prendre des mesures raisonnables et appropriées pour protéger ces données.

Sécurité des données dans le secteur public

► Réduire l'utilisation inutile du numéro d'assurance sociale dans le secteur public en élaborant des stratégies de rechange pour la gestion de l'identité.
- Faire un relevé des usages courants du NAS par le gouvernement fédéral.
- Publier des lignes directrices sur les utilisations appropriées du NAS.
- Créer un centre d'information sur les pratiques « exemplaires » des organismes qui minimisent l'utilisation du NAS.
- Examiner les usages du NAS en collaboration avec les gouvernements étatiques et locaux.

► Informer les organismes fédéraux de la façon de protéger les données, et surveiller le respect des lignes directrices existantes.
- Préparer des lignes directrices concrètes et des pratiques exemplaires.
- Surveiller la façon dont les organismes respectent les lignes directrices.
- Protéger les dispositifs de stockage et de communication de données.

► Garantir des mesures d'intervention efficaces axées sur le risque en cas de brèches dans la

guarding Data
- Hold regional seminars for businesses on safeguarding information
- Distribute improved guidance for private industry

► Initiate Investigations of Data Security Violations

► Initiate a Multi-Year Public Awareness Campaign
- Develop national awareness campaign
- Enlist outreach partners
- Increase outreach to traditionally underserved communities
- Establish "Protect Your Identity" Days

► Develop Online Clearinghouse for Current Educational Resources

PREVENTION: MAKING IT HARDER TO MISUSE CONSUMER DATA

Because security systems are imperfect and thieves are resourceful, it is es-sential to reduce the opportunities for criminals to misuse the data they steal. An identity thief who wants to open new accounts in a victim's name must be able to (1) provide identifying information to allow the creditor or other grantor of benefits to access information on which to base a decision about eligibility; and (2) convince the creditor that he is the person he purports to be.

Authentication includes determining a person's identity at the beginning of a relationship (sometimes called verification), and later ensuring that he is the same person who was originally authenticated. But the process can fail: Identity documents can be falsified; the accuracy of the initial information and the accuracy or quality of the verifying sources can be questionable; employee training can be insufficient; and people can fail to follow procedures.

Efforts to facilitate the development of better ways to authenticate consum-ers without burdening consumers or businesses—for example, multi-factor authentication or layered security—would go a long way toward preventing criminals from profiting from identity theft.

► Hold Workshops on Authentication
- Engage academics, industry, entrepre-

protection des données confiées au sein d'organismes fédéraux.
- Émettre aux organismes des lignes directrices en cas de brèches dans la protection des données.
- Publier « un mode d'emploi courant » autorisant la divulgation d'information aux entités, après une brèche, afin de les aider à réagir à l'incident.

Sécurité des données dans le secteur privé

► Établir des normes nationales concernant la protection des données par le secteur privé et la notification des brèches dans la protection des données.

► Établir un dossier complet sur l'utilisation des numéros d'assurance sociale par le secteur privé.

► Mieux renseigner le secteur privé sur la protection des données.
- Tenir à l'intention des entreprises des séminaires régionaux sur la protection des renseignements.
- Offrir un meilleur encadrement à l'industrie privée.

► Faire enquête en cas de brèches dans la protection des données.

► Entreprendre une campagne de sensibilisation du public étalée sur plusieurs années.
- Élaborer une campagne de sensibilisation nationale.
- S'assurer de la participation de partenaires.
- Accroître la sensibilisation des collectivités habituellement mal desservies.
- Établir des journées de « protection de votre identité ».

► Créer un centre d'information en direct concernant les ressources éducatives courantes.

PRÉVENTION : RENDRE PLUS DIFFICILE L'UTILISATION MALVEILLANTE DES DONNÉES SUR LES CONSOMMATEURS

Étant donné que les systèmes de sécurité sont

neurs, and government experts on developing and promoting better ways to authenticate identity
- Issue report on workshop findings

► Develop a Comprehensive Record on Private Sector Use of SSNs

VICTIM RECOVERY: HELPING CONSUMERS REPAIR THEIR LIVES

Identity theft can be committed despite a consumer's best efforts at securing information. Consumers have a number of rights and resources available, but some surveys indicate that they are not as well-informed as they could be. Government agencies must work together to ensure that victims have the knowledge, tools, and assistance necessary to minimize the damage and begin the recovery process.

► Provide Specialized Training About Victim Recovery to First Responders and Others Offering Direct Assistance to Identity Theft Victims
- Train law enforcement officers
- Provide educational materials for first responders that can be used as a reference guide for identity theft victims
- Create and distribute an ID Theft Victim Statement of Rights
- Design nationwide training for victim assistance counselors

► Develop Avenues for Individualized Assistance to Identity Theft Victims

► Amend Criminal Restitution Statutes to Ensure That Victims Recover the Value of Time Spent in Trying to Remediate the Harms Suffered

► Assess Whether to Implement a National System That Allows Victims to Obtain an Identification Document for Authentication Purposes

► Assess Efficacy of Tools Available to Victims
- Conduct assessment of FACT Act remedies under FCRA
- Conduct assessment of state credit freeze laws

imparfaits et que les voleurs sont très astucieux, il est essentiel de réduire les occasions pour les criminels d'utiliser à mauvais escient les données qu'ils volent. Un voleur d'identité qui veut ouvrir de nouveaux comptes au nom d'une victime doit être en mesure : 1) de fournir des renseignements de base qui permettent au créancier ou autre prestataire d'avantages de consulter l'information nécessaire pour prendre une décision sur l'admissibilité, et 2) de convaincre le créancier que la personne est bel et bien celle qu'elle prétend être.

Pour authentifier une personne, on doit déterminer son identité au début d'une relation (processus parfois appelé vérification) et, plus tard, s'assurer qu'il s'agit bien de la même personne qui a été authentifiée au départ. Cependant, les pièces d'identité peuvent avoir été falsifiées, l'exactitude des premiers renseignements et la précision et la qualité des sources de vérification peuvent être douteuses, la formation de l'employé peut être insuffisant, et les gens en poste peuvent négliger de suivre les procédures.

Les efforts déployés pour faciliter l'élaboration de meilleures façons d'authentifier les consommateurs sans imposer de fardeau aux consommateurs comme aux entreprises – par exemple, un mécanisme d'authentification ou des mesures de sécurité à plusieurs niveaux – contribueraient grandement à empêcher les criminels de commettre un vol d'identité.

► Organiser des ateliers sur l'authentification.
  - Inciter les universitaires, les industriels, les entrepreneurs et les spécialistes du gouvernement à élaborer de meilleures méthodes d'authentification et à en faire la promotion.
  - Publier un rapport sur les conclusions des ateliers.

► Établir un registre complet de l'utilisation des NAS par le secteur privé.

RÉTABLISSEMENT DES VICTIMES: AIDER LES CONSOMMATEURS À SE REMETTRE

Le vol d'identité peut survenir malgré les efforts déployés par les consommateurs pour protéger leurs renseignements. Les consommateurs ont des droits et des ressources, mais certaines enquêtes démontrent qu'ils ne sont pas aussi bien

LAW ENFORCEMENT: PROSECUTING AND PUNISHING IDENTITY THIEVES

Strong criminal law enforcement is necessary to punish and deter identity thieves. The increasing sophistication of identity thieves in recent years has meant that law enforcement agencies at all levels of government have had to increase the resources they devote to investigating related crimes. The inves-tigations are labor-intensive and generally require a staff of detectives, agents, and analysts with multiple skill sets. When a suspected theft involves a large number of potential victims, investigative agencies often need additional personnel to handle victim-witness coordination.

Coordination and Information / Intelligence Sharing

► Establish a National Identity Theft Law Enforcement Center

► Develop and Promote the Use of a Universal Identity Theft Report Form

► Enhance Information Sharing Between Law Enforcement and the Private Sector
  - Enhance ability of law enforcement to receive information from financial institutions
  - Initiate discussions with financial services industry on countermeasures to identity theft
  - Initiate discussions with credit reporting agencies on preventing identity theft

Coordination with Foreign Law Enforcement

► Encourage Other Countries to Enact Suitable Domestic Legislation Criminalizing Identity Theft

► Facilitate Investigation and Prosecution of International Identity Theft by Encouraging Other Nations to Accede to the Convention on Cybercrime

► Identify the Nations that Provide Safe Havens for Identity Thieves and Use All Measures Available to Encourage Those Countries to Change Their Policies

► Enhance the United States Government's Ability to Respond to Appropriate Foreign Requests for Evidence in Criminal Cases Involv-

informés qu'on pourrait le croire. Les organismes du gouvernement devraient collaborer entre eux pour s'assurer que les victimes ont les connaissances, l'aide et les outils requis pour minimiser les dommages et amorcer le processus de rétablissement.

► Offrir une formation spécialisée sur le rétablissement des victimes aux premiers intervenants et à ceux qui fournissent une aide directe pour reconnaître les victimes de vol d'identité.
  - Former les agents d'exécution de la loi.
  - Fournir aux premiers intervenants du matériel pédagogique pouvant servir de référence pour reconnaître les victimes de vol d'identité.
  - Élaborer et distribuer un énoncé des droits des victimes de vol d'identité.
  - Concevoir un programme national de formation à l'intention des conseillers chargés d'aider les victimes.

► Concevoir des façons d'offrir une aide personnalisée aux victimes de vol d'identité.

► Modifier la législation sur la restitution des produits de la criminalité pour que les victimes récupèrent la valeur correspondant au temps perdu à corriger les torts subis.

► Déterminer s'il y a lieu de mettre en œuvre un système national qui permette aux victimes d'obtenir une pièce d'identité aux fins d'authentification.

► Évaluer l'efficacité des outils mis à la disposition des victimes.
  - Évaluer les mesures correctives de la FACT Act en vertu de la FCRA.
  - Évaluer la situation des lois des États concernant le resserrement du crédit.

EXÉCUTION DE LA LOI : POURSUIVRE ET PUNIR LES VOLEURS D'IDENTITÉ

Une application musclée de la loi s'impose pour punir et dissuader les voleurs d'identité. Le raffinement croissant des méthodes employées par les voleurs d'identité ces dernières années a obligé les organismes d'exécution de la loi à tous les niveaux du gouvernement à augmenter les ressources consacrées aux enquêtes sur les crimes. Les enquêtes exigent beaucoup de main-

ing Identity Theft

► Assist, Train, and Support Foreign Law Enforcement

Prosecution Approaches and Initiatives

► Increase Prosecutions of Identity Theft
  - Designate an identity theft coordinator for each United States Attorney's Office to design a specific identity theft program for each district
  - Evaluate monetary thresholds for prosecution
  - Encourage state prosecution of identity theft
  - Create working groups and task forces

► Conduct Targeted Enforcement Initiatives
  - Conduct enforcement initiatives focused on using unfair or deceptive means to make SSNs available for sale
  - Conduct enforcement initiatives focused on identity theft related to the health care system
  - Conduct enforcement initiatives focused on identity theft by illegal aliens

► Review Civil Monetary Penalty Programs

Gaps in Statutes Criminalizing Identity Theft

► Close the Gaps in Federal Criminal Statutes Used to Prosecute Identity Theft-Related Offenses to Ensure Increased Federal Prosecution of These Crimes
  - Amend the identity theft and aggravated identity theft statutes to ensure that identity thieves who misappropriate information belonging to corporations and organizations can be prosecuted
  - Add new crimes to the list of predicate offenses for aggravated identity theft offenses
  - Amend the statute that criminalizes the theft of electronic data by eliminating the current requirement that the information must have been stolen through interstate communications
  - Penalize creators and distributors of malicious spyware and keyloggers
  - Amend the cyber-extortion statute to cover additional, alternate types of cyber-extortion

d'œuvre et supposent habituellement un personnel composé de détectives, d'agents et d'analystes ayant de nombreuses compétences. Dès qu'un vol touche un grand nombre de victimes éventuelles, les organismes d'enquête doivent recourir à du personnel supplémentaire pour assurer la coordination des victimes et des témoins.

Coordination et partage de renseignements

► Établir un centre national d'application de la loi en matière de vol d'identité.

► Élaborer un formulaire universel de déclaration de vol d'identité et en promouvoir l'utilisation.

► Améliorer le partage de renseignements entre la police et le secteur privé.
- Améliorer la capacité des responsables de l'exécution de la loi d'obtenir des renseignements des établissements financiers.
- Amorcer des discussions avec l'industrie des services financiers concernant des mesures de prévention du vol d'identité.
- Amorcer des discussions avec les agences d'évaluation du crédit concernant la prévention du vol d'identité.

Coordination avec des organismes d'exécution de la loi de l'étranger

► Encourager d'autres pays à adopter une législation intérieure pour criminaliser le vol d'identité.

► Faciliter les enquêtes sur le vol d'identité à l'échelle internationale et les poursuites en incitant les autres pays à accéder à la Convention sur la cybercriminalité.

► Recenser les pays qui offrent asile aux voleurs d'identité et utiliser tous les moyens disponibles pour inciter ces pays à modifier leurs politiques.

► Mettre en valeur la capacité du gouvernement des États-Unis de donner suite aux demandes de l'étranger de preuves appropriées dans les affaires au criminel concernant le vol d'identité.

► Aider, former et soutenir les responsables de

► Ensure That an Identity Thief's Sentence Can Be Enhanced When the Criminal Conduct Affects More Than One Victim

Law Enforcement Training

► Enhance Training for Law Enforcement Officers and Prosecutors
- Develop course at National Advocacy Center focused on investigation and prosecution of identity theft
- Increase number of regional identity theft seminars
- Increase resources for law enforcement on the Internet
- Review curricula to enhance basic and advanced training on identity theft

Measuring the Success of Law Enforcement

► Enhance the Gathering of Statistical Data Impacting the Criminal Justice System's Response to Identity Theft
- Gather and analyze statistically reliable data from identity theft victims
- Expand scope of national crime victimization survey
- Review U.S. Sentencing Commission data
- Track prosecutions of identity theft and resources spent
- Conduct targeted surveys

l'exécution de la loi.

Approche aux poursuites et initiatives

► Augmenter le nombre de poursuites pour vol d'identité.
- Nommer un coordonnateur du vol d'identité pour chacun des bureaux du Procureur des États-Unis chargés de concevoir un programme particulier sur le vol d'identité pour chacun des districts.
- Évaluer le seuil monétaire à partir duquel entamer des poursuites.
- Encourager les États à entamer des poursuites en cas de vol d'identité.
- Constituer des groupes de travail.

► Mener des initiatives ciblées d'exécution de la loi.
- Mener des activités d'exécution de la loi axées sur l'utilisation de moyens injustes ou trompeurs pour faciliter la vente des NAS.
- Mener des activités d'exécution de la loi axées sur le vol d'identité en rapport avec le système de soins de santé.
- Mener des activités d'exécution de la loi axées sur le vol d'identité par des étrangers clandestins.

► Examiner les programmes d'amendes civils.

Lacunes de la législation criminalisant le vol d'identité

► Corriger les lacunes de la législation fédérale servant de base aux poursuites en matière d'offenses reliées au vol d'identité pour faire en sorte que ces crimes fassent l'objet d'un nombre accru de poursuites fédérales.
- Modifier les lois concernant le vol d'identité et le vol qualifié d'identité afin que les voleurs d'identité qui s'approprient illégalement des renseignements appartenant à des corporations et à des organisations puissent faire l'objet de poursuites.
- Ajouter de nouvelles offenses à la liste existante pour les cas de vol qualifié d'identité.
- Modifier les lois qui criminalisent le vol de données électroniques en éliminant l'obligation courante selon laquelle les renseignements doivent avoir été volés dans le cadre de communications entre

États.

- Sanctionner les créateurs et les distributeurs de logiciels espions et d'enregistreurs de frappe.
- Modifier la loi concernant la cyberextorsion pour couvrir d'autres types de cyberextorsions.

► S'assurer de la possibilité d'accroître la peine d'un voleur d'identité lorsque le crime touche plus d'une victime.

Formation en matière d'exécution de la loi

► Améliorer la formation des agents d'exécution de la loi et des procureurs
- Élaborer un cours au centre national de défense des intérêts axé sur les enquêtes et sur les poursuites en cas de vol d'identité.
- Augmenter le nombre de séminaires régionaux sur le vol d'identité.
- Accroître les ressources d'exécution de la loi dans Internet.
- Examiner les programmes en vue d'améliorer la formation de base et la formation avancée portant sur le vol d'identité.

Mesure du succès de l'exécution de la loi

► Améliorer la collecte de données statistiques sur les conséquences pour le système de justice pénale des interventions à la suite de vols d'identité.
- Recueillir et analyser des données statistiques fiables provenant de victimes de vol d'identité.
- Élargir la portée de l'enquête nationale sur les victimes de la criminalité.
- Examiner le rendement de la commission américaine sur la détermination de la peine.
- Faire un relevé des poursuites pour vol d'identité et des ressources consacrées à ces cas.
- Mener des enquêtes ciblées.

29^E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Qui vous espionne lorsque vous utilisez votre ordinateur ?

Who’s Spying on Your Computer?

National Network to End Domestic Violence



AVERTISSEMENT DE SÉCURITÉ : Il y a longtemps que le harcèlement existe, mais il est plus facile que jamais pour les auteurs de ce crime de harceler, de suivre et de surveiller leur victime. Les gens qui se livrent à la violence, au harcèlement ou à d'autres crimes peuvent maintenant utiliser un logiciel espion pour surveiller ce que fait une personne lorsqu'elle utilise son ordinateur ou un appareil portatif, par exemple un téléphone cellulaire, sans qu'elle le sache. Si vous pensez que quelqu'un vous surveille ou si vous vous sentez traqué, vous devez savoir les choses suivantes :

- il pourrait être dangereux pour vous d'essayer de détecter un logiciel espion installé sur votre ordinateur, appareil portatif ou téléphone cellulaire, parce que la personne qui vous surveille peut savoir immédiatement que vous effectuez des recherches en ce sens;

- vous devez utiliser un ordinateur ou un appareil portatif sécuritaire (un appareil auquel la personne qui vous surveille n'a pas accès directement ou à distance) pour effectuer des recherches dans Internet ou pour envoyer des courriels que vous ne voulez pas que la personne puisse lire;

- si vous voulez conserver des preuves de l'installation d'un logiciel espion dans votre ordinateur, veuillez communiquer avec le service de police de votre ville.

Pour consulter des listes de logiciels et d'appareils espions qui sont faciles à installer dans un ordinateur et qui peuvent être utilisés pour espionner un amant, une petite amie, un petit ami, un partenaire, un mari ou une femme et pour surveiller en secret l'utilisation que fait une épouse infidèle de son ordinateur, il suffit de taper « espionner sa femme » dans n'importe quel moteur de recherche.

QU'EST-CE QU'UN LOGICIEL ESPION?

Un logiciel espion est un logiciel informatique ou un appareil qui permet à une personne (mal intentionnée) de surveiller en secret l'utilisation qu'une autre personne fait de son ordinateur et de recueillir des renseignements de cette façon, sans y être autorisée.

Il existe de nombreux types de logiciels informatiques et d'appareils qu'on peut installer dans un ordinateur pour surveiller l'utilisation qui

SAFETY ALERT: While stalking is an age-old crime, Spyware has made it easier than ever before for perpetrators to stalk, track, monitor, and harass their victims. Abusers, stalkers and other perpetrators can now use Spyware to secretly monitor what you do on your computer or handheld device, like a cell phone. If you suspect you are being stalked or monitored, be aware that:

- Attempting to look for spyware on your computer or handheld/phone could be dangerous since the abuser could be alerted to your searches immediately

- Use a safer computer or handheld device (one that the stalker does not have remote or physical access to) to perform Internet searches or send emails that you wouldn't want an abuser to intercept

- If you want to preserve evidence of Spyware on your computer, contact your local police, a domestic

Simply type, "spy on girlfriend" into any search engine, and instantly see listings and links advertising easy-to-install computer Spyware programs and devices that can be used to "spy on a lover, girlfriend, boyfriend, partner, husband or wife and secretly record computer activities to catch a cheating spouse."

WHAT IS SPYWARE?

Spyware, is a computer software program or hardware device that enables an unauthorized person (such as an abuser) to secretly monitor and gather information about your computer use.

There are many types of computer software programs and hardware devices that can be installed to monitor your computer activities. They can be installed on your computer without your knowledge, and the person installing them doesn't even need to have physical access to your computer. Whether computer monitoring is legal or illegal depends on the state you live in, and the context in which it is installed and used. Regardless of the legality, Spyware is invasive, intrusive, and may put victims in grave danger.

Spyware programs are sometimes marketed as ways to monitor your children or your employees. As an employer, it is always best to have your

en est faite. Quelqu'un peut installer ces appareils ou logiciels dans votre ordinateur sans que vous le sachiez, sans même nécessairement avoir directement accès à votre ordinateur. La surveillance informatique est légale dans certains États, illégale dans d'autres, et cela dépend aussi du contexte dans lequel le logiciel ou l'appareil est installé et utilisé. Dans tous les cas, les logiciels espions sont importuns, envahissants et peuvent représenter un grand danger pour les victimes.

Les logiciels espions sont parfois présentés par les entreprises qui les vendent comme le moyen de surveiller des enfants ou des employés. Si vous êtes un employeur, vous devriez demander à vos employés de lire et de signer une politique d'utilisation des outils technologiques. Cette politique devrait expliquer les utilisations permises des biens de l'entreprise, définir les attentes quant aux gestes qui peuvent être posés en ligne, et en INFORMER les employés lorsque leur ordinateur fait l'objet d'une surveillance. En outre, vous devriez choisir un progiciel qui affiche une icône rappelant aux employés qu'ils sont surveillés. (*Voir aussi la remarque à l'intention des parents à la fin du présent texte.)

Il existe certaines ressemblances et différences entre les logiciels espions et les logiciels connexes. Voici quelques exemples :

- **Logiciel publicitaire** : Il s'agit de logiciels de marketing cachés qui affichent des publicités sur les écrans des consommateurs, qui peuvent aussi servir à établir le profil des utilisateurs d'Internet quant à leurs habitudes de navigation et de magasinage. Les logiciels publicitaires sont souvent cachés dans un autre logiciel téléchargé par un utilisateur, ou encore en font partie. La plupart des ordinateurs ordinaires sont touchés par les logiciels publicitaires assez régulièrement, et les signes courants sont notamment le ralentissement du système et beaucoup de fenêtres flash publicitaires.

- **Logiciel malveillant** : Il s'agit de tout programme qui tente de s'installer dans un système informatique de lui‑même ou de l'endommager sans le consentement du propriétaire. Ce sont notamment des virus, des vers, des logiciels espions et des logiciels publicitaires.

Pour de plus amples renseignements sur les logiciels publicitaires et malveillants, veuillez

employees read and sign a "Technology Use Policy." This policy should explain allowable uses of company property, expectations of online behavior, and TELL employees if their computer will be monitored. Additionally, choose a software package that displays an icon to remind your employees that they're being monitored. (* Also - see note to parents at the end of this piece).

There are some similarities and differences between Spyware and its close relatives.. For example:

- **Adware**: These are hidden marketing programs that deliver advertising to consumers, and might also profile users' Internet surfing & shopping habits. Adware is often bundled or hidden in something else a user downloads. Most average computer users are infected with adware fairly regularly, and common symptoms include a sluggish system and lots of advertising pop-ups.

- **Malware**: This is any program that tries to install itself or damage a computer system without the owner's consent. Malware includes viruses, worms, spyware and adware.

For more information on adware and malware, see "Protecting Your Computer" at www.antispywarecoalition.org/documents/documents/ProtectingYourComputerflyerletter.pdf

HOW DOES SPYWARE WORK?

Spyware can keep track of every keystroke you type, every software application you use, every website you visit, every chat or instant message you send, every document you open, and everything you print. Some spyware gives the abuser the ability to freeze, shutdown or restart your computer. Some versions even allow the abuser to remotely turn on your webcam or make your computer talk.

Once Spyware is installed, it can run in stealth mode and is difficult to detect or uninstall. If the person who installed it has physical access to your computer, he or she can use a special key combination that will cause a log-in screen to pop-up. After entering the password, an options screen will pop up that allows the installer to view all of the computer activity since their last login, including emails you sent, documents printed,

consulter le document intitulé « Protecting Your Computer » à l'adresse suivante : www.antispywarecoalition.org/documents/documents/ProtectingYourComputerflyerletter.pdf (en anglais seulement).

COMMENT LES LOGICIELS ESPIONS FONCTIONNENT-ILS?

Les logiciels espions permettent de surveiller tout ce que vous saisissez au clavier, toute utilisation d'une application logicielle que vous faites, tous les sites Web que vous visitez, toutes les séances de clavardage auxquelles vous participez, tous les messages instantanés que vous envoyez, tous les documents que vous ouvrez et tout ce que vous imprimez. Certains logiciels espions permettent à la personne qui l'utilise de geler votre ordinateur, de l'éteindre ou de le redémarrer. Certaines versions de ces logiciels permettent même d'activer votre caméra Web à distance ou de faire parler votre ordinateur.

Une fois qu'un logiciel espion est installé, il peut fonctionner en mode furtif et être difficile à détecter ou à désinstaller. Si la personne qui l'a installé a directement accès à votre ordinateur, elle peut utiliser une combinaison de touches particulières pour faire afficher un écran d'ouverture de session. En saisissant le mot de passe, elle fait ensuite afficher une fenêtre qui lui permet de prendre connaissance de tout ce que vous avez fait avec votre ordinateur depuis la dernière session, notamment les courriels que vous avez envoyés, les documents que vous avez imprimés, les sites Web que vous avez visités, etc. Si la personne n'a pas directement accès à votre ordinateur, elle peut demander au logiciel espion d'effectuer des saisies de votre écran à intervalles de quelques secondes et de les lui envoyer par Internet sans que vous le sachiez.

Exemples d'activités informatiques qui peuvent facilement faire l'objet d'une surveillance :

Voir la figure en annexe

COMMENT UN LOGICIEL ESPION PEUT-IL SE RETROUVER DANS MON ORDINATEUR?

La personne qui veut vous surveiller peut installer un logiciel espion dans votre ordinateur ou un appareil portatif que vous possédez si elle y a

websites visited, and more. Perpetrators without physical access to your computer can set the spyware to take pictures of the computer screen (screen shots) every few seconds and have these pictures sent to them over the Internet without a victim's knowledge.

See the example in the appendix

HOW DOES IT GET ON MY COMPUTER?

Abusers can install Spyware on your computer if they have physical or Internet access to your computer or handheld device. Some abusers might hack into your computer from another location via the Internet. Some might send spyware to you as an attached file that automatically installs itself when you open the email or when you initially view it in a preview window. Others may email or instant message a greeting card, computer game, or other ruse in order to entice you or your children to open an attachment or click on a link. Once opened, the program automatically installs spyware on the victim's computer, in stealth mode without notification or consent, and can then send electronic reports to the perpetrator via the Internet.

While most spyware is software based (a program that can be installed on your computer), there are also some hardware-based spyware devices called keystroke loggers. These tiny keylogging devices may appear to be a normal computer part. However, once the keylogger is plugged into your computer, it can record every key typed, capturing all passwords, personal identification numbers (PIN), websites visited, and any emails sent onto its small hard drive. Additionally, there are keyboards with keystroke logging capabilities built-i

Note: Remember that many handheld devices are mini-computers. There are now spyware programs available for cell phones and other handheld devices, so that the perpetrator can track every text message sent and every phone number dialed. (note: phone records can also be obtained by non-spyware methods, such as guessing your account password and accessing your account on the phone company website, or by viewing your call history stored in the phone.)

directement accès ou si elle y a accès par Internet. Certaines personnes peuvent accéder à votre ordinateur à distance par Internet. Il se peut aussi qu'on vous envoie un logiciel espion comme pièce jointe qui s'installe automatiquement lorsque vous ouvrez le courriel ou que vous l'affichez dans une fenêtre d'aperçu. Autre possibilité : on peut vous faire parvenir par courriel ou par message instantané une carte de souhait ou un jeu, ou encore utiliser une autre tactique pour vous inciter à ouvrir une pièce jointe ou à cliquer sur un lien, ou encore inciter vos enfants à le faire. Une fois ouvert, le programme installe automatiquement un logiciel espion dans l'ordinateur de la victime, en mode furtif, sans avis ou sans le consentement de la victime, et le logiciel espion peut ensuite envoyer des rapports électroniques à la personne qui en est à l'origine par Internet.

La plupart des outils d'espionnage informatique sont des logiciels (il s'agit de programmes qu'on installe dans un ordinateur), mais il y a aussi des appareils qui remplissent la même fonction et qu'on appelle des enregistreurs de frappe. Ces petits appareils qui enregistrent la frappe peuvent sembler faire partie de l'ordinateur. Cependant, lorsque l'appareil est branché à votre ordinateur, il est en mesure d'enregistrer sur un petit disque dur ce que vous saisissez au clavier, tous les mots de passe, numéros d'identification personnels (NIP), tous les sites Web que vous visitez et tous les courriels que vous envoyez. Il existe en outre des claviers qui permettent d'enregistrer la frappe.

Remarque : N'oubliez pas que de nombreux appareils portatifs sont de mini-ordinateurs. Il existe maintenant des logiciels espions pour les téléphones cellulaires et les autres appareils portatifs, qui permettent à une personne de surveiller les messages-textes que vous envoyez et les numéros de téléphone que vous composez. (Remarque : Il est aussi possible d'obtenir le registre d'appels autrement qu'à l'aide d'un logiciel espion, par exemple en devinant votre mot de passe et en accédant à votre compte de services téléphoniques sur le site Web du fournisseur, ou encore en consultant l'historique d'appels de votre téléphone.)

COMMENT FAIRE POUR SAVOIR SI UN LOGICIEL ESPION EST INSTALLÉ DANS MON ORDINATEUR?

- Si votre ordinateur est actuellement sous surveillance, il peut être dangereux pour vous d'essayer de détecter un logiciel espion ou

HOW DO I FIND OUT IF THERE'S SPYWARE ON MY COMPUTER?

- If your computer is currently being monitored it may be dangerous to try to research spyware or use anti-spyware scanners. If your computer is compromised, spyware will log all of this research activity and alert the perpetrator.

- If you suspect that someone has installed spyware to monitor your activities, talk to a victim advocate before attempting to remove the spyware. Law enforcement or a computer forensics expert may be able to assist you if you want to preserve evidence that may be needed for a criminal investiga

Spyware typically runs in stealth mode using disguised file names so it can be extraordinarily difficult to detect spyware programs that are already on your computer.

While your computer is being monitored by Spyware there might be no noticeable changes in the way your computer operates (i.e. your computer won't necessarily slow down or freeze up). Also, like computer viruses, there are hundreds of Spyware programs. So while some are created by large software companies, other spyware programs are written by individual "hackers".

There are a variety of programs marketed as Anti-Spyware detectors that primarily identify Adware and Malware, but may not discover surveillance Spyware. Additionally, anti-spyware detection programs typically does not detect hardware, like keystroke loggers.

If you think there may be spyware on your computer, consider the tips below:

TIPS FOR SURVIVORS OF ABUSE

- If you use the monitored computer to try to research spyware or try to access anti-spyware scanners, spyware will log all of this activity and alert the perpetrator which could be dangerous.

- Try to use a safer computer when you look for domestic or sexual violence resources. It may be safer to use a computer at a public library, community center, or Internet café.

d'utiliser un logiciel qui sert à repérer les logiciels espions. Si votre ordinateur est touché, le logiciel espion enregistre toutes vos tentatives de recherche et alerte la personne qui vous surveille.

- Si vous pensez que quelqu'un a installé un logiciel espion pour surveiller vos activités, consultez un défenseur des droits des victimes avant d'essayer de désinstaller le logiciel espion. La police ou encore un expert judiciaire en informatique pourront peut-être vous aider si vous souhaitez conserver des preuves qui pourraient être nécessaires dans le cadre d'une enquête criminelle.

En général, les logiciels espions fonctionnent en mode furtif et utilisent des noms de fichiers fictifs, ce qui fait qu'il est extrêmement difficile de détecter ces logiciels lorsqu'ils sont installés dans un ordinateur.

Si un logiciel espion est installé dans votre ordinateur et surveille votre utilisation de celui-ci, il se peut que vous ne remarquiez aucun changement dans le fonctionnement de l'ordinateur (c.-à-d. que l'ordinateur ne va pas nécessairement ralentir ou geler). Par ailleurs, tout comme dans le cas des virus informatiques, il existe des centaines de logiciels espions différents. Ainsi, certains logiciels sont créés par de grandes entreprises de logiciels, mais d'autres le sont par des « pirates informatiques ».

Il y a sur le marché toutes sortes de logiciels qui servent à détecter les logiciels espions, mais ceux-ci servent surtout à détecter les logiciels publicitaires et les logiciels malveillants, sans pour autant nécessairement permettre de découvrir un logiciel espion utilisé pour surveiller quelqu'un. En outre, les logiciels de détection des logiciels espions ne permettent généralement pas de détecter les appareils comme les enregistreurs de frappe.

Si vous pensez qu'un logiciel espion est installé dans votre ordinateur, les conseils qui suivent s'adressent à vous.

CONSEILS POUR LES SURVIVANTS

- Si vous utilisez l'ordinateur sous surveillance pour essayer de détecter les logiciels espions installés dans celui-ci ou pour essayer de

- If you suspect that anyone abusive can access your email or Instant Messaging (IM), consider creating additional email/IM accounts on a safer computer. Do not create or check new email/IM accounts from a computer that might be monitored. Look for free web-based email accounts, and strongly consider using non-identifying name & account information. (example: bluecat@email.com and not YourRealName@email.com) Also, make sure to carefully read the registration screens so you can choose not to be listed in any online directories.

- Be suspicious if someone abusive has installed a new keyboard, cord, or software, or recently or done computer repair work that coincides with an increase of stalking or monitoring.

- If you are thinking about buying a new computer, there are steps you can take to reduce the chance of spyware getting on your new machine but it is impossible to eliminate the risk.
  - Install and enable a firewall. There are both software and hardware firewalls. If a firewall didn't come with your computer, you can download a software one for free from www.zonealarm.com.
  - Have at least one anti-virus protection program installed and actively scanning your computer, and make sure your anti-virus definitions are up-to-date because new dangerous viruses are released daily. This may involve setting your computer to automatically updates its virus definitions and run anti-virus scans daily and making sure to renew your anti-virus software subscription every year.
  - Install anti-spyware programs before you even connect to the Internet and make sure their spyware definitions are updated automatically and regularly.

- Trust your instincts and look for patterns. If your abuser knows too much about things you’ve only told people via email or instant messenger, there may be spyware on your computer. If you think you’re being monitored by an abuser, you probably are.

télécharger un logiciel de détection de logiciels espions, le logiciel espion consignera toutes vos activités et alertera la personne qui vous surveille, ce qui peut être dangereux.

- Vous devriez chercher à utiliser un ordinateur sécuritaire lorsque vous consultez des ressources sur la violence conjugale ou sexuelle. Il serait plus sûr que vous utilisiez un ordinateur dans une bibliothèque publique, un centre communautaire ou un cybercafé.

- Si vous pensez qu'une personne mal intentionnée a accès à vos courriels ou à votre service de messagerie instantanée (MI), vous devriez envisager de créer de nouveaux comptes de courriel/de MI à partir d'un ordinateur sécuritaire. N'ouvrez pas de nouveaux comptes et ne prenez pas de messages à partir d'un ordinateur si vous pensez qu'il peut être sous surveillance. Privilégiez les comptes de courriel Web et les noms et renseignements sur votre compte qui ne permettent pas de vous identifier, (p. ex., chatbleu@courriel.com et non votrevrainom@courriel.com). Par ailleurs, assurez-vous de bien lire le contenu des écrans d'inscription, de façon à pouvoir choisir d'exclure votre nom des répertoires en ligne.

- Méfiez-vous si une personne ayant un comportement violent a installé un nouveau clavier, un nouveau câble ou un nouveau logiciel, ou encore a récemment réparé votre ordinateur et que cela coïncide avec une surveillance ou une impression d'être traqué plus importante qu'auparavant.

- Si vous songez faire l'acquisition d'un nouvel ordinateur, il y a des mesures que vous pouvez prendre pour réduire le risque qu'un logiciel espion soit installé dans votre nouvel ordinateur, même s'il est impossible d'éliminer totalement les risques.
  - Installez un pare-feu et activez-le. Il existe des pare-feu sous forme de logiciels et d'appareils. Si votre ordinateur n'est pas muni d'un pare-feu intégré, vous pouvez télécharger un logiciel à l'adresse suivante : www.zonealarm.com.
  - Installez au moins un logiciel antivirus dans votre ordinateur afin qu'il cherche activement des virus qui peuvent être dans votre ordinateur et

Can't I just "clear" and "delete" my history or trail?

- It is not possible to clear the traces on the computer, especially since Spyware will record all of your attempts to clear your many computer histories. There are literally hundreds of histories hidden in the computer. Also, an abuser may become suspicious and escalate control if he/she has been monitoring your computer history and activities for a while and then one day sees empty histories.

- Spyware records everything you do on the computer or device, and then records all your attempts to delete your computer activities. Sometimes, Spyware is impossible to detect without a forensic examination of your hard drive or unless you know the password and keycode your abuser uses to view screenshots of your computer activities.

- Attempting to clear your histories, trying to find whether Spyware is installed on your computer, or reaching out for help through a domestic violence webpage could be dangerous on a computer that your stalker or abuser is monitoring.

TIPS FOR ORGANIZATIONS THAT ASSIST VICTIMS

Post a Safety Alert on every page of your Website

- Posting a clear, but brief safety alert can make victims aware of risks. (Example: "Your computer activities might be impossible to erase. If someone might be monitoring you, please use a safer computer or call a hotline for more information.)

Take steps to increase your organization's data security.

- Organizations should protect any personally identifiable information collected about a victim since any data leaks or breaches could be fatal. For safety reasons, we recommend that organizations not store confidential or personally-identifiable information about a victim on any computer that is connected to the Internet. Without an internet connection, there is significantly less risk that an abuser will hack in and access your organization's data, or, that a virus will infect your computer and automatically emailing confidential files out to others.

assurez-vous que les définitions de virus du logiciel sont à jour, puisque de nouveaux virus dangereux sont libérés quotidiennement. Il se peut que vous deviez demander à votre ordinateur d'effectuer de façon automatique les mises à jour des définitions de virus et d'effectuer des recherches de virus quotidiennes. Assurez-vous de renouveler votre abonnement au logiciel antivirus tous les ans.

  - Installez des logiciels servant à détecter des logiciels espions avant même d'effectuer une connexion à Internet et assurez-vous que les définitions de logiciels espions de ces logiciels sont mises à jour de façon automatique et régulière.

- Fiez-vous à votre intuition et cherchez à détecter des régularités. Si la personne qui vous surveille sait des choses que vous n'avez dites qu'à des gens par courriel ou par messagerie instantanée, votre ordinateur est peut-être infecté par un logiciel espion. Si vous pensez qu'une personne vous surveille, c'est probablement parce que c'est le cas.

Pourquoi ne puis-je me contenter de « supprimer » mon historique de navigation?

- Il est impossible d'effacer toute trace de navigation dans votre ordinateur, surtout parce que les logiciels espions enregistrent toutes vos tentatives de suppression des nombreux historiques qui figurent dans votre ordinateur. En réalité, il y a des centaines d'historiques cachés dans votre ordinateur. Par ailleurs, la personne qui vous surveille peut se méfier et vous surveiller de plus près si elle suit vos activités et votre historique depuis un moment et s'aperçoit tout à coup que vos historiques de navigation sont vides.

- Les logiciels espions enregistrent tout ce que vous faites avec votre ordinateur ou avec votre appareil, puis enregistrent toutes vos tentatives de suppression des traces de vos activités. Dans certains cas, les logiciels espions sont impossibles à détecter à moins de demander à un spécialiste d'effectuer un examen de votre disque dur et à moins de connaître le mot de passe et la combinaison de touches que la personne qui vous surveille

- It is important to have organizational policies that address electronic and paper information practices including who can or can't access certain data, and the secure disposal of confidential papers, computer hard drives, and other electronic media (i.e. external or USB hard drives) that contain victim data. For a data security checklist see: www.nnedv.org/SafetyNet/Publications/NNEDV_DataSecurityHandout.pdf

Carefully consider computer safety issues before contemplating providing services via the Internet

- Know the facts! 60-80% of computers are infected with viruses, adware, or other malware which can compromise the safety of both the victim/survivor and your agency's computers. (www.pewinternet.org)

- Know that you cannot guarantee the safety and/or security of the computer of every person who uses your services. Provide upfront and complete disclosures to service users about safety, confidentiality and capacity issues so they can make realistic and informed choices about use.

- Provide information about the technology, confidentiality and security limits of online service provision, including disparities in access to technology varied internet speeds and internet connection outages.

- Discuss in your organization the potential harm that could come to victims if an abuser is monitoring a victim's entire escape plan that the victim shares through online service provision.

Use Firewalls and keep Anti-Virus & Anti-Spyware Definitions Updated

- As always, updated protection software is the first line of defense against Malware and Adware. However, these programs offer limited protections against surveillance spyware, since monitoring software can appear to be a legitimate product and might not be flagged by these programs. Regardless of the precautions a user takes, spyware allows an abuser to monitor computer and Internet activities and discover a victim's efforts to escape or access help.

utilise pour visualiser les saisies d'écran effectuées pour surveiller votre ordinateur.

- Il peut être dangereux pour vous de tenter d'effacer vos historiques, d'essayer de déterminer si un logiciel espion est installé dans votre ordinateur ou d'essayer d'obtenir de l'aide en consultant une page Web sur la violence conjugale, si vous utilisez un ordinateur surveillé par une personne mal intentionnée.

CONSEILS POUR LES ORGANISATIONS QUI VIENNENT EN AIDE AUX VICTIMES

Affichez un avertissement de sécurité sur toutes les pages de votre site Web

- Vous pouvez aider les victimes à prendre conscience des risques en affichant un avertissement de sécurité clair, mais bref, dans votre site Web (p. ex. : « Il se peut que vous soyez incapable de supprimer les traces d'utilisation de votre ordinateur. Si vous pensez que quelqu'un vous surveille, utilisez un ordinateur sécuritaire ou composez le numéro d'une ligne d'aide pour obtenir de plus amples renseignements. »)

Prenez des mesures pour sécuriser les données qui sont en possession de votre organisation

- Les organisations devraient protéger tout renseignement personnel sur une victime qui permet de l'identifier, puisqu'une fuite ou une brèche dans la protection des données pourrait engendrer des conséquences graves pour cette personne. Pour des raisons de sécurité, nous recommandons aux organisations de ne pas conserver de renseignements confidentiels ou qui permettent d'identifier une victime dans les ordinateurs branchés à Internet. Avec les ordinateurs qui ne sont pas connectés à Internet, le risque qu'une personne mal intentionnée s'infiltre et accède aux données de votre organisation, ou encore qu'un virus infecte l'ordinateur et envoie à l'extérieur des fichiers confidentiels par courriel de façon automatique, est beaucoup moins important.

- Il est important que l'organisation établisse des politiques sur les pratiques relatives à l'information en format électronique ou papier,

Secure your Computers

- Make sure all of your agency's computers require strong alphanumeric passwords to log in. Each user should have a different password, and they should not use the name of your organization, your address, or any similar information.

- If you have computers that are for public use, consider setting them so that users cannot download software.

TIPS FOR PARENTS

- After educating yourself about the Internet and computers, have a conversation with your children about the Internet and its benefits and risks. Together, come up with a set of Internet safety rules for your family. If your children take part in creating the rules, they will be more likely to follow them.

- Keep the family computer in a public space like the family room or living room. If your children know that you could walk past at any moment, they're much less likely to break your agreed upon rules.

- If you choose to use Parental Monitoring Software: TELL your child that you will be using it and explain why. Building trust and respect around computer use is extremely important, so that your children will feel comfortable coming to you if an issue or problem does arise. Also look for one that displays an icon somewhere on the screen while in use. The icon will help children remember that they're being watched and encourage them to follow your Internet safety rules.

notamment en ce qui concerne les personnes autorisées à accéder à telle ou telle donnée, la façon sécuritaire de se débarrasser des documents confidentiels, des disques durs d'ordinateurs et d'autres outils électroniques (p. ex., les disques durs externes ou les clés USB) qui contiennent des données sur les victimes. Veuillez consulter la liste de vérification de la sécurité des données à l'adresse suivante : www.nnedv.org/SafetyNet/Publications/NNEDV_DataSecurityHandout.pdf (en anglais seulement).

Assurez-vous de régler les questions relatives à la sécurité informatique avant d'envisager d'offrir des services dans Internet

- Prenez connaissance des faits : de 60 à 80 p. 100 des ordinateurs sont infectés par des virus, des logiciels publicitaires ou d'autres logiciels malveillants qui peuvent compromettre la sécurité à la fois des victimes/des survivants et des ordinateurs de votre organisation. (www.pewinternet.org)

- Prenez conscience du fait que vous ne pouvez garantir la sécurité des ordinateurs de toutes les personnes qui utilisent vos services. Informez bien et dès le départ les utilisateurs de vos services au sujet des questions de sécurité, de confidentialité et de capacité, de façon qu'ils puissent prendre des décisions éclairées et réalistes avant d'utiliser vos services.

- Fournissez des renseignements sur les limites des outils technologiques, de la confidentialité et de la sécurité qu'offrent les services en ligne, notamment en ce qui concerne les différences d'accès aux outils technologiques, les différentes connexions à Internet (rapidité) et les pannes de connexion.

- Discutez, au sein de votre organisation, du préjudice que peuvent subir les victimes dans le cas où la personne qui leur veut du mal sait exactement comment la victime prévoit lui échapper, parce que celle-ci en a discuté dans le cadre de services en ligne.

Utilisez des pare-feu et assurez-vous de mettre à jour les définitions de virus et de logiciels espions

- Évidemment, la première chose à faire pour se protéger des logiciels malveillants et des

logiciels publicitaires est de mettre à jour ses logiciels de protection. Cependant, ces programmes offriront une protection limitée contre les logiciels utilisés pour la surveillance, puisque ceux-ci peuvent passer pour des produits légitimes et ne pas être repérés par des logiciels de détection. Même si l'utilisateur prend des précautions, le logiciel espion permet à la personne qui lui veut du mal de le surveiller lorsqu'il utilise son ordinateur et navigue dans Internet, ce qui lui permet de savoir ce que sa victime fait pour essayer de lui échapper ou d'obtenir de l'aide.

Sécurisez vos ordinateurs

- Assurez-vous que l'ouverture d'une session sur tous les ordinateurs de votre organisation exige un mot de passe alphanumérique offrant un haut niveau de sécurité. Chaque utilisateur devrait avoir un mot de passe qui lui est propre, et les utilisateurs ne devraient pas utiliser à cette fin le nom de votre organisation, votre adresse ou des renseignements du genre.

- Si vous avez des ordinateurs publics, envisagez de bloquer le téléchargement de logiciels par les utilisateurs.

CONSEILS POUR LES PARENTS

- Après vous être renseigné sur Internet et sur les ordinateurs, discutez avec vos enfants des avantages qu'offre Internet et des risques qui existent. Avec les membres de votre famille, établissez un ensemble de règles de sécurité pour la navigation dans Internet. Si vos enfants participent à la création des règles, ils seront plus susceptibles de les respecter.

- Placez l'ordinateur familial dans un espace partagé, par exemple dans la pièce familiale ou le salon. Si vos enfants savent que vous pouvez passer devant l'ordinateur à tout moment, ils seront beaucoup moins susceptibles d'enfreindre les règles établies.

- Si vous décidez d'utiliser le logiciel de surveillance parentale, DITES à vos enfants que vous allez le faire et expliquez-leur pourquoi. Il est extrêmement important que vous permettiez l'utilisation de l'ordinateur dans un climat de confiance et de respect, de façon que vos enfants soient à l'aise de vous

faire part de tout problème qui pourrait survenir. Par ailleurs, vous devriez utiliser un logiciel qui affiche une icône à l'écran lorsqu'il est activé. Ainsi, vos enfants se rappelleront qu'ils sont surveillés, et cela va les encourager à respecter les règles de sécurité pour la navigation dans Internet.

Annexe / Appendix

One example of the types of computer activity that can be easily monitored:





LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

La haute technologie et ses méfaits : Technologie, traque et activités de défense

A High-Tech Twist on Abuse: Technology, Intimate Partner Stalking, and Advocacy

Safety Net



Remerciements

L'équipe du projet Safety Net (projet de filet de sécurité) désire signaler l'aide précieuse qu'elle a reçue de Beth Zagorski, de Pam Shea, du Stalking Resource Center au National Center for Victims of Crime et des nombreux membres de groupes de défense qui ont contribué à la préparation de ce document et qui, jour après jour, soutiennent des survivantes.

Introduction

> *[Traduction]*
> *« L'autoroute de l'information qui parcourt notre monde est une arme à double tranchant pour les survivantes. Une survivante qui veut fuir un agresseur n'a pas d'autre objectif que de fuir. Et quelle horreur quand, après avoir réussi à fuir, et souvent avec de jeunes enfants à la remorque, elle découvre qu'en réalité la fuite est impossible. Avec Internet, impossible de se cacher. » --- Survivante du Texas*

La traque d'un partenaire intime n'est pas un phénomène nouveau. Par contre, les progrès technologiques mettent à la disposition des traqueurs une toute nouvelle panoplie d'outils. En effet, les traqueurs peuvent maintenant se servir des diverses technologies que sont les appareils téléphoniques, les appareils de surveillance et les ordinateurs pour surveiller et harceler leurs partenaires intimes, actuelles ou passées. Certains agresseurs installent des systèmes de positionnement mondial pour localiser leur victime en temps réel avec une extraordinaire précision, alors que d'autres se servent du téléphone pour leur laisser des centaines de messages par jour. D'autres encore utilisent les bases de données en ligne, les dossiers électroniques et les moteurs de recherche du Web pour localiser, traquer et harceler d'ex-partenaires. Les méthodes et les choix technologiques des traqueurs peuvent varier, mais les survivantes sont nombreuses à le signaler : la traque et les agressions dont elles font l'objet ont pris une allure hautement technologique.

Dans ce document, on examinera les nouvelles méthodes utilisées par les traqueurs, on donnera des conseils importants pour planifier sa sûreté et on proposera des mesures aux services locaux

Acknowledgements

The Safety Net Team wishes to thank and acknowledge assistance with this paper from Beth Zagorski, Pam Shea, the Stalking Resource Center at the National Center for Victims of Crime, and the many advocates that helped birth this paper and support survivors every day.

Introduction

> *"The information superhighway world we live in is a two-edge [sic] sword for survivors. The whole goal of escaping an abuser is to do just that, escape. After one has gone through the trauma of leaving, often with small children in tow, how horrifying it is to wake up to the reality that you can't escape at all. The Internet doesn't hide anyone." ---Survivor in Texas*

Intimate partner stalking is not a new phenomenon. However, the ongoing advancement of technology is providing stalkers with a sophisticated selection of tools. Stalkers are using a variety of telephone, surveillance, and computer technologies to monitor and harass current and former intimate partners. Some abusers install global positioning systems to discover their victim's real-time location with extraordinary accuracy, while others use telephones to leave hundreds of messages in a single day. Still others use online databases, electronic records, and web search engines to locate, track, and harass former partners. While stalkers' methods and choice of technologies vary, survivors report that they are experiencing stalking and abuse that is perpetrated with a high-tech twist.

This paper presents information regarding new methods used to stalk, important safety planning tips, and action steps for local programs working to end violence against women. Advocates are encouraged to learn about these new stalking methods, expand traditional approaches to safety planning, and enhance the community response to victims of intimate partner stalking. The tips presented are not meant to read as a universally prescribed course of action. This paper offers many safety planning strategies, however the safest course of action may vary in each individual situation. Though many survivors of stalking are

d'intervention contre la violence faite aux femmes. On invite les groupes de défense à prendre connaissance de ces nouvelles méthodes de traque, à élargir leurs approches traditionnelles de la planification de la sûreté et à améliorer la façon des groupes communautaires de venir en aide aux victimes des partenaires intimes traqueurs. Les conseils présentés ici ne constituent en aucun cas une règle à suivre en toutes circonstances. Dans ce document figurent de nombreuses stratégies de planification de la sûreté, mais leur validité dépend de la situation. S'il est vrai que les survivantes font preuve de plus en plus de créativité dans leur utilisation de la technologie pour renforcer leur sécurité, ce document porte sur l'utilisation que font les agresseurs des technologies nouvelles et existantes.

Les termes employés dans ce document introduisent de nouvelles idées qui viennent compléter les notions qu'on a déjà de la violence faite aux femmes et de la traque. Comme les personnes qui ont survécu à des cas d'agression utilisent différents termes pour se désigner, on utilisera indifféremment dans le présent document les termes « survivante » ou « victime ». On utilisera aussi indifféremment les termes « traqueur », « agresseur » et « harceleur » pour parler des partenaires intimes auteurs de violence – catégorie regroupant la violence familiale, la violence sexuelle et la traque d'une conjointe ou ex-conjointe, d'une ancienne petite amie ou d'une personne proche (Greenfeld *et al*, 1998).

Recherche et portée

Depuis 15 ans à peine, le système juridique reconnaît que la traque est un acte criminel et le traite comme tel. L'État de la Californie a été le premier du pays à adopter, en 1990, une loi contre la traque, à la suite du meurtre très médiatisé de l'actrice Rebecca Schaeffer qu'un trop fervent admirateur avait traquée et du cas de traque beaucoup moins connu de cinq femmes du comté d'Orange par d'anciens partenaires intimes qui ont fini par les assassiner (Gilligan, 1992, cité dans Jenson, 1996). Pendant la décennie qui a suivi, les 50 États des États-Unis, le District fédéral de Columbia et le gouvernement fédéral ont fini par adopter des lois qui criminalisent la traque (Stalking Resource Center, 2003). Malgré leurs variations, de ces lois on peut tirer une définition générale de la traque : il s'agit du

creatively using technology to increase their safety, this paper focuses on perpetrators' use of emerging and existing technologies.

Terms in this paper convey new ideas that build on existing knowledge of violence against women and stalking. Since people surviving abuse identify themselves differently, the terms "victim" and "survivor" are used interchangeably. "Stalker," "abuser," and "offender" are also used interchangeably to reference perpetrators of intimate partner violence -- a category encompassing domestic violence, sexual violence, and stalking that targets a current or former spouse, boyfriend, girlfriend, or significant other (Greenfeld et al., 1998).

Research and Scope

Only in the past 15 years has the legal system begun to recognize and address the crime of stalking. California passed the nation's first anti-stalking state law in 1990, following the highly publicized stalking and murder of actress Rebecca Schaeffer by a fan, and the much less publicized stalking and murder of five Orange County women by former intimate partners (Gilligan, 1992 as cited in Jenson, 1996). Over the next decade, anti-stalking laws were passed in all 50 states, the District of Columbia, and at the federal level (Stalking Resource Center, 2003). Despite some variation, these laws helped frame a general definition of stalking as "a course of conduct directed at a specific person that would cause a reasonable person fear" (National Center for Victims of Crime, 2004, p. 1).

The National Violence Against Women Survey (NVAW) begins to document the prevalence of stalking crimes by reporting that 1.4 million people are stalked annually and, by conservative estimates, at least 1 in 12 women and 1 in 45 men has been stalked at some point in their lives. Over three quarters (78%) of stalking victims are female and most (87%) stalking perpetrators are male (Tjaden &Thoennes, 1998).

Research indicates a clear link between stalking and intimate partner violence. Nationally studies show that former husbands, boyfriends, or cohabitating partners perpetrate a majority (62%) of the stalking incidents against females (Department of Justice, 2001). Of women stalked by current or former partners, eighty-one percent

[traduction] « comportement adopté à l'endroit d'une certaine personne pour lui faire raisonnablement craindre pour sa sécurité » (National Center for Victims of Crime, 2004, p. 1).

L'enquête appelée National Violence Against Women Survey (NVAW) commence à documenter l'importance de la traque en révélant que 1,4 million de personnes aux États-Unis sont traquées par année et que, selon des estimations prudentes, au moins une femme sur 12 et 1 homme sur 45 sont traqués à un moment donné dans leur vie. Plus des trois quarts (78 %) des victimes de traque sont des femmes et la majorité des traqueurs (87 %) sont des hommes (Tjaden & Thoennes, 1998).

Les recherches effectuées révèlent également qu'il existe un lien évident entre la traque et la violence par un partenaire intime. Des études réalisées à l'échelle nationale indiquent que la majorité (62 %) des traques signalées contre des femmes sont le fait d'ex-conjoints, amis ou partenaires vivant sous le même toit (Department of Justice, 2001). Parmi les femmes traquées par leurs partenaires ou ex-partenaires, 81 % ont été agressées physiquement et 31 % l'ont été sexuellement par le partenaire en question (Department of Justice, 2001). Il existe aussi un lien étroit entre la traque et le risque d'être assassiné par un partenaire intime. Dans une analyse des meurtres de femmes par leur partenaire intime, il apparaît que, dans 76 % des cas de meurtre, l'assassin avait traqué au moins une fois sa victime (McFarlane *et al*, 1999). Certains experts sont même allés jusqu'à dire que [traduction] « si la traque est définie comme un comportement qui intimide ou effraie la victime, alors les relations marquées par la violence familiale relèvent aussi de la traque » (National Center for Victims of Crime, 2004, p. 2).

De nouvelles technologies et le caractère beaucoup plus accessible de celles-ci ouvrent aux traqueurs un éventail inédit d'outils pour terroriser leurs partenaires intimes, actuelles ou anciennes. [traduction] « La révolution de l'information a grandement élargi la portée des technologies de l'intrusion » et, par le fait même, « l'arsenal du traqueur » (Spitzberg et Hoobler, 2002, p. 72). À la fin de 2003, 63 % des adultes américains se servaient d'Internet (Madden et Rainie, 2003). À la fin de décembre 2002, quelque 102 millions d'Américains se servaient du courrier électronique

were physically assaulted and 31% were sexually assaulted by that same partner (Department of Justice, 2001). Stalking is also interconnected with the risk of being murdered by an intimate; in one review of women killed by intimate partners, 76% of the murders were preceded by one or more incidents of stalking (McFarlane, et al., 1999). Experts have even argued that "If stalking is defined as a course of conduct that intimidates or frightens the victim, then relationships involving domestic violence also involve stalking" (National Center for Victims of Crime, 2004, p.2).

New forms of technology and increased access to technology provide stalkers with new tools to terrorize current or former intimate partners. "The information revolution has vastly increased the scope of technologies of intrusion" and thus "expanded the arsenal of the stalker" (Spitzberg &Hoobler, 2002, p.72). As of late 2003, 63% of adult Americans were using the Internet (Madden &Rainie, 2003). As of December 2002, about 102 million Americans were email users (Madden &Rainie, 2003). While it is difficult to determine the prevalence of technology use by intimate partner stalkers, qualitative evidence — testimony from survivors and highlights from representative research studies, convenience samples, and anecdotal cases — indicates an urgent need to address safety risks for victims while concurrently assessing the extent and prevalence of technology misuse.

Awareness of technology harassment began in the mid-1990s, when Internet users began reporting online harassment and threats. This use of technology was labeled "cyberstalking". A 1999 U.S. Congressional Report defines cyberstalking as "the use of the Internet, e-mail, or other electronic communications devices to stalk another person" (Department of Justice, 1999, What Is Cyberstalking section, para 1). Others have defined cyberstalking more broadly to include the use of electronic communication including pagers, cell phones, emails and the Internet, to bully, threaten, harass, and intimidate a victim (Laughren, 2000; Ellison &Akdeniz, 1998; CyberAngels, 1999; Dean, 2000; Ogilvie, 2000; Maxwell, 2001). A 1998 study noted, "electronic stalking often leads to, or is accompanied by, physical stalking, and explicitly or implicitly threatens physical stalking" (Lee, 1998, p. 391). To recognize the full range of technologies, stalking experts are moving away from the term "cyberstalking" and beginning to use "the use of

(Madden et Rainie, 2003). S'il est difficile de cerner la place de la technologie dans les méthodes des partenaires intimes traqueurs, les données qualitatives – témoignages des survivantes et conclusions d'études représentatives, échantillons de commodité et rapports sur des cas isolés – signalent un urgent besoin de se pencher sur les risques pour la sécurité des victimes tout en évaluant parallèlement l'importance du mauvais emploi de la technologie.

C'est vers le milieu des années 1990 qu'on a pris conscience de l'existence d'une nouvelle forme de harcèlement : le harcèlement technologique. Les utilisateurs d'Internet ont commencé à cette époque-là à signaler des problèmes de harcèlement et de comportements menaçants en ligne. C'est ce qu'on a appelé la « cybertraque ». Le terme a même été défini dans un rapport du Congrès américain de 1999 comme étant [traduction] « l'utilisation d'Internet, du courriel et d'autres appareils de communication électroniques pour traquer quelqu'un » (Department of Justice, 1999, rubrique *What Is Cyberstalking?*, par. 1). D'autres ont défini la « cybertraque » plus largement pour inclure l'utilisation des communications électroniques, y compris les téléavertisseurs, les téléphones cellulaires, le courriel et Internet, pour intimider, menacer et harceler une victime (Laughren, 2000; Ellison et Akdeniz, 1998; CyberAngels, 1999; Dean, 2000; Ogilvie, 2000; Maxwell, 2001). Dans une étude de 1998, l'auteur indiquait que [traduction] « la cybertraque s'accompagne souvent d'une traque physique ou bien mène à elle, et constitue donc une menace explicite ou implicite de traque physique » (Lee, 1998, p. 391). Pour bien reconnaître tout l'éventail des technologies utilisées, les experts de la traque préfèrent s'éloigner du concept de « cybertraque » pour parler plutôt de l'« utilisation de la technologie pour traquer » (Bahm, 2003, p. 2).

Si aucune étude exhaustive n'a été menée, plusieurs travaux n'en signalent pas moins certains types de technologies utilisées par les traqueurs. En particulier, certains chercheurs ont noté l'utilisation du téléphone, du courriel et de la messagerie instantanée. Ainsi, dans une enquête réalisée auprès des femmes traquées par d'ex-partenaires intimes, plus de 90 % ont déclaré avoir reçu des coups de téléphone de leur agresseur (Brewster, 2003). Les auteurs d'une étude nationale des victimes de traque ont trouvé

technology in stalking" (Bahm, 2003, p.2).

While there are no comprehensive studies, several reports document specific technology types used by stalkers. In particular, certain studies have recorded the use of telephones, email, and instant messaging in stalking. For example, in a survey of women stalked by former intimate partners, over 90% reported telephone calls from their stalker (Brewster, 2003). A national study of stalking victims found that females (62%) were significantly more likely than males (42%) to receive repeated unwanted telephone calls from their stalker (Finn, 2004). Unfortunately, data is limited, and the few studies that record telephone use in stalking do not report information about the type of telephones (e.g. cell, cordless), telephone-related technologies (e.g. pagers) or integrated location and surveillance devices (e.g. cameras, global positioning systems).

Popular culture often focuses on cyberstalking via email and instant messaging and some studies document these methods of stalking. As early as 1997, a nationally representative study of students attending 223 U.S. colleges and universities reported that 13.1% of female students were stalked during the first seven months of the 1996-1997 school year; nearly 25% of these victims reported being stalked via email (Fisher, Cullen, &Turner, 2000). At least 20% of the cases reported in a 1999 survey of criminal justice and investigation units involved email or electronic communications and electronic harassment or threats (Department of Justice, 1999). The organization Working to Halt Online Abuse (WHOA) discovered that 58% of the people who contacted them for support in 2003 knew their harasser previously, and 57% of the harassers were former partners (WHOA, 2003). In a recent randomized, convenience sample of University of New Hampshire undergraduate students, 9.6% of students surveyed reported receiving threats, insults, or harassment from significant others via email, and 11% received threats through instant messages (Finn, 2004).

To date, there are no nationally representative studies that explore the breadth of information, communications, and surveillance technologies being used in intimate partner stalking. Additional research is needed to examine the extent to which various technologies are being used to stalk victims of intimate partner violence. Survivors

que les femmes risquaient davantage que les hommes, dans une proportion de 62 % contre 42 %, de recevoir des appels téléphoniques répétés et non désirés de leur traqueur (Finn, 2004). Malheureusement, on a peu de données sur la question et les rares études qui évaluent l'utilisation du téléphone dans les affaires de traque ne font pas de distinction sur le genre d'appareil téléphonique utilisé (cellulaire ou sans fil, par exemple) ou ne précisent pas si l'agresseur a recouru à des technologies liées à la téléphonie (téléavertisseurs) ou à des appareils intégrés de localisation et de surveillance (comme des caméras ou des systèmes de positionnement mondial).

Dans la culture populaire, on associe le plus souvent la « cybertraque » au courriel et à la messagerie instantanée, et ces méthodes figurent effectivement au nombre de celles utilisées par les traqueurs selon certaines études. Dès 1997, une étude représentative à l'échelle nationale réalisée auprès d'étudiants de 223 collèges et universités des États‑Unis a révélé que 13,1 % des étudiantes avaient été traquées pendant les sept premiers mois de l'année scolaire 1996-1997, dont 25 % avaient déclaré l'avoir été par courriel (Fisher, Cullen et Turner, 2000). Au moins 20 % des cas signalés dans une enquête des services de justice pénale et d'enquête criminelle de 1999 mettaient en cause le courriel ou les communications électroniques et le harcèlement ou des menaces électroniques (Department of Justice, 1999). L'organisation Working to Halt Online Abuse (WHOA) a découvert que 58 % des personnes qui s'étaient adressées à elle en 2003 pour obtenir de l'aide connaissaient leur harceleur et que 57 % des harceleurs étaient effectivement d'anciens partenaires de leurs victimes (WHOA, 2003). Selon un récent échantillon de commodité randomisé des étudiants de premier cycle de l'université de New Hampshire, 9,6 % des étudiants sondés auraient déclaré avoir reçu des menaces ou des insultes ou avoir été harcelés par un proche au moyen du courriel, et 11 % auraient dit avoir reçu des menaces par message instantané (Finn, 2004).

Jusqu'à présent, aucune étude représentative n'a été faite à l'échelle nationale pour évaluer l'éventail des technologies de l'information, des communications et de la surveillance utilisées dans les affaires de traque par des partenaires intimes. Il faudrait d'autres recherches pour évaluer l'importance des diverses technologies

would greatly benefit if future violence against women research addressed the context and use of specific technologies in intimate partner violence and stalking. Additional qualitative research would enhance survivor safety by identifying appropriate and useful system and community responses.

Stalkers use numerous technology and non-technology tools to stalk, monitor, and intimidate their victims. Advocates must learn about and address these high-tech tactics, but always in the larger context of a victim's stalking experience. As Tracy Bahm, the Director of the Stalking Resource Center in Washington, D.C. states, "No matter what tools they use, stalkers are still stalkers" (Bahm, 2003, p.2).

The Use of Technology to Stalk

Survivors report that stalkers are using many forms of technology - old and new - to control, coerce, and intimidate them during and after relationships. Some stalkers inundate former intimate partners with "dozens of emails and instant messages, often using automated senders and anonymous remailers that make it hard to identify the source" (Lamberg, 2001, Cyberstalking: A Growing Threat section, para 2). Other stalkers use technologies such as caller ID during a relationship to monitor their partner's calls, and to locate her after she has fled.

This paper includes highlights of some of the common abuses of technology, including a sampling of survivor stories collected by Safety Net: the National Safe and Strategic Technology Project at 191 training sessions to over 10,000 advocates, law enforcement officers, and allies. This section begins with telephone technologies, continues with global positioning systems, hidden cameras, computer monitoring devices, and ends with online databases. Advocacy tips are also included to provide options for addressing survivor safety issues. As existing technologies are changing and new technologies are emerging, these strategies provide an adaptable starting point for advocates to include technology in current safety planning efforts.

Telephone Technologies

Abusers regularly use telephone technologies to

dans les méthodes utilisées par les partenaires intimes pour traquer leurs victimes. Les survivantes gagneraient certainement beaucoup à ce que la recherche future sur la violence faite aux femmes se penche sur le contexte et l'utilisation de technologies précises dans les affaires de violence familiale et de traque par un partenaire intime. D'autres études qualitatives permettraient de renforcer la sécurité des survivantes en les aidant à trouver des solutions systémiques et communautaires utiles.

Les traqueurs se servent de nombreux outils technologiques et autres pour traquer, surveiller et intimider leurs victimes. Les groupes de défense doivent apprendre à connaître ces tactiques qui reposent sur la haute technologie et à y réagir, mais toujours dans le contexte plus vaste de l'expérience de traque de la victime. Comme l'a rappelé Tracy Bahm, directrice du Stalking Resource Center à Washington, D.C., [traduction] « peu importe les outils qu'ils utilisent, les traqueurs restent des traqueurs! » (Bahm, 2003, p. 2).

La technologie au service du traqueur

Les survivantes indiquent que les traqueurs utilisent de nombreuses formes de technologies, nouvelles et anciennes, pour exercer leur contrôle, faire pression sur leur victime et les intimider, pendant la relation et après. Certains traqueurs envoient à leurs ex-partenaires des [traduction] « douzaines de courriels et de messages instantanés, souvent au moyen d'expéditeurs automatisés et de réexpéditeurs anonymes qui rendent difficile l'identification de la source » (Lamberg, rubrique *Cyberstalking: A Growing Threat*, 2001, par. 2). D'autres se servent de technologies comme la fonction d'identification de l'appelant pour surveiller les appels de leur partenaire et la retrouver si elle réussit à fuir.

Dans ce document, on met en lumière certains des usages abusifs courants de la technologie, en renvoyant à l'occasion aux histoires de survivantes recueillies par le Safety Net: the National Safe and Strategic Technology Project durant 191 séances de formation données à plus de 10 000 intervenants de groupes de défense, agents d'application de la loi et leurs alliés. Divisé en trois sections, ce chapitre du document traite en premier lieu des appareils téléphoniques, en deuxième lieu des systèmes de positionnement

stalk current and former intimate partners (Brewster, 2003). While most homes have traditional telephones, many families are also using cellular and wireless telephones, creating a new realm of tools for stalkers to use. In June 2004, approximately 169 million Americans used wireless telephones (Cellular Telecommunications &Internet Association, 2004). As wireless telephones become more sophisticated, abusers are finding ways to use advanced telephone features to aid them in stalking their victims. However, abusers have also found creative ways to stalk with even the most basic telephone technologies.

Telephones. Abusers commonly stalk through repeated and harassing telephone calls, sometimes using prepaid calling cards or prepaid cell phones that leave minimal information trails. If a phone card is not activated with a credit card, linked to a discount card, or billed to a person's long distance phone carrier, the harassing call can be difficult to trace. Perpetrators also leave threatening messages in voicemail and on answering machines.

Caller ID. Caller Identification (Caller ID) is a popular tool that abusers may use to monitor their victim's telephone calls while in the relationship, and to stalk and locate their victim after the relationship has ended. Caller ID devices provide the name and number of the caller, and some even provide the address of the caller. In 1995, soon after caller ID was first available, an abuser tracked down and subsequently murdered his former girlfriend by using caller ID (Associated Press, 1995).

Fax Machines. Abusers and stalkers have used the fax header on faxed documents to locate their victims. New fax machines also contain caller ID, creating additional safety challenges for survivors. In one example, a woman fled, but had to send papers to her abusive partner. She faxed the papers from the shelter fax machine to her attorney. Her attorney faxed the papers to his attorney. His attorney gave the papers to him. Since no one removed the fax header, the abuser acquired the telephone number and location of his victim and she had to relocate again (Safety Net, 2004).

TTY/TTD. Teletypewriters (TTY) and Telecommunications Devices for the Deaf (TTD) are text based telephones that people who are

mondial, des caméras cachées et des appareils de surveillance informatique et, en troisième lieu, des bases de données en ligne. Il contient aussi des conseils à l'intention des groupes de défense pour les aider à trouver différents moyens d'assurer la sécurité des survivantes. À mesure qu'évoluera la technologie, les stratégies proposées serviront de point de départ à l'élaboration d'autres stratégies adaptées qui tiendront compte de la technologie dans les efforts de planification de la sécurité des survivantes.

Appareils téléphoniques

Les agresseurs utilisent régulièrement le téléphone pour traquer leur partenaire ou ex-partenaire intime (Brewster, 2003). Si la plupart des foyers ont des téléphones traditionnels, nombreuses sont les familles qui disposent également de téléphones cellulaires et de téléphones sans fil, ouvrant ainsi la porte à un monde d'outils nouveaux pour le traqueur. En juin 2004, quelque 169 millions d'Américains se servaient de téléphones sans fil (Cellular Telecommunications and Internet Association, 2004). Ces téléphones, qui deviennent de plus en plus perfectionnés, offrent aux traqueurs de nouveaux moyens de traquer leur victime. Mais même avec un téléphone tout ce qu'il y a de plus traditionnel, les agresseurs ont aussi réussi à parfaire leurs méthodes.

Téléphones. Les traqueurs choisissent souvent de faire des appels téléphoniques répétés et harassants en utilisant parfois des cartes d'appel ou des téléphones cellulaires prépayés qui laissent peu de traces. Si une carte d'appel n'est pas activée avec une carte de crédit, liée à une carte de rabais ou facturée au service téléphonique interurbain, il peut être difficile de retracer l'origine de l'appel. Les traqueurs laissent aussi souvent des messages de menaces dans le courriel vocal et sur les répondeurs.

Identification de l'appelant. La fonction d'identification de l'appelant est bien connue et appréciée des traqueurs qui s'en servent pour surveiller les appels téléphoniques de leur victime alors qu'ils sont encore avec elle, et pour traquer et localiser leur victime une fois la relation rompue. Les dispositifs d'identification de l'appelant donnent le nom et le numéro de l'appelant, et même parfois son adresse. En 1995, peu après que ces appareils ont fait leur

deaf or hard of hearing use to communicate. These devices often record and save an exact history of conversations, making it easier for stalkers to monitor victims' conversations. Abusers also impersonate victims by using their TTY to seek information about her activities. In one case, a prosecutor working with a Deaf victim got a call on his TTY, allegedly from the victim, reading, "If you don't drop the charges against my boyfriend, I'm going to kill myself." When help was sent to the victim's home it was found that she had been sleeping when the TTY call was made. The abuser had impersonated the victim in an attempt to persuade the prosecutor to withdraw charges (Safety Net, 2004).

Cellular &Wireless Telephones. Abusers can monitor their victims' cell or wireless telephone use through the call history on the telephone and through billing records. Most cell phones keep an internal record of incoming and outgoing calls. Stalkers also use phone-based instant messaging, simple text messaging, and pagers to maintain constant access to their intimate partners. Stalkers can use new location based services provided by cell phone carriers to track the location of their victims. In Rhode Island one abuser assaulted his wife after finding the shelter telephone number in her cell phone call history; as a result she did not attempt to leave her husband for another year (Safety Net, 2004).

Location & Surveillance Technologies

Stalkers are increasingly using basic and sophisticated location and imaging technology to conduct surveillance, thus putting victims' safety at great risk. Before abusers had access to location tracking devices like global positioning systems, they often checked car odometers to measure mileage and monitor victims' daily activities. Now, tools ranging from inexpensive digital cameras to high-tech streaming video cameras and global positioning systems, while not inherently surveillance devices, are being used as such by perpetrators.

Global Positioning Systems. Abusers use Global Positioning Systems (GPS) that use satellite receivers to provide precise real-time worldwide positioning, to locate and follow victims. These devices vary by price, size, and appearance. GPS may appear as a small black box, a hand-held unit, or even a small chip in a

apparition sur le marché, un agresseur a traqué puis assassiné son ancienne amie en utilisant ce type d'appareil (Associated Press, 1995).

Télécopieurs. Des agresseurs et des traqueurs se sont déjà servis des pages de présentation de documents envoyés par télécopie pour retrouver leur victime. Les nouveaux télécopieurs ont aussi une fonction d'identification de l'appelant, ce qui multiplie les risques pour les survivantes. Dans une certaine affaire, une femme avait fui, mais devait envoyer des papiers à son ex-partenaire abusif. Elle a envoyé les papiers par télécopieur, du refuge où elle était, à son avocat qui, lui, les a télécopiés à l'avocat de l'agresseur. Quand le client de celui-ci a récupéré les documents dont personne n'avait supprimé la page de présentation, il a pris connaissance du numéro de téléphone et de l'adresse de sa victime qui a dû déménager à nouveau (Safety Net, 2004).

TTY/TTD. Les téléimprimeurs (TTY) et les appareils de télécommunication pour sourds (TTD) sont des téléphones qui émettent des textes écrits pour les personnes atteintes de surdité ou les malentendants. Ces appareils enregistrent souvent pour les conserver un historique exact des conversations, ce qui fait qu'il est plus facile pour le traqueur de surveiller les conversations de sa victime. Les traqueurs usurpent également l'identité de leur victime en utilisant leur TTY pour obtenir des renseignements sur les activités de celle-ci. Dans une certaine affaire, un avocat qui travaillait avec un client sourd a reçu un appel sur son TTY, soi disant de la victime. Le texte de l'appel se lisait comme suit [traduction] : « Si tu ne retires pas tes accusations contre mon ami, je vais me suicider. » Quand l'avocat a envoyé quelqu'un chez la victime pour l'aider, il s'est avéré qu'elle dormait au moment de l'appel. L'agresseur s'était fait passer pour elle dans l'espoir de persuader l'avocat de retirer ses accusations (Safety Net, 2004).

Téléphones cellulaires et sans fil. Les agresseurs peuvent surveiller l'utilisation que fait leur victime du téléphone cellulaire ou sans fil en vérifiant l'historique des appels du téléphone ou les factures. La plupart des téléphones cellulaires conservent un registre interne des appels qui arrivent et qui sortent. Les agresseurs se servent aussi de la messagerie téléphonique instantanée, de la messagerie textuelle simple et des téléavertisseurs pour garder contact à tout

wristband. Global positioning technology can also be part of anti-theft services for vehicles such as OnStar. In December 2002, a Wisconsin man secretly installed a GPS device under the hood of his ex-girlfriend's car and stalked her for months. "He would follow her as she drove to work or ran errands. He would inexplicably pull up next to her at stoplights and once tried to run her off the highway" (Orland, 2003, para 2). Since GPS devices are becoming cheaper and smaller as technology advances, it is imperative that survivors are educated about the ways to check for such devices.

Hidden Cameras. Stalkers use small hidden cameras to monitor their victims and learn their routines. Stalkers use information they gather to exert power and control over their victims. Small wireless high-resolution cameras can be hidden in smoke detectors, children's lamps, or behind a pin-sized hole in a wall, and can even be activated remotely. In 2003, the Supreme Court of New Jersey found that a defendant's video surveillance of his estranged wife in her bedroom presented a prima facie case of stalking and harassment under the New Jersey Domestic Violence Act (H.E.S. v. J.C.S., 2003).

Computer & Internet Technology

Abusers continue to identify and adapt new computer software and hardware tools that allow them to further stalk and harass their victims. They not only use low-technology monitoring options such as viewing the website browser history or intercepting email, but also are increasingly using more sophisticated SpyWare software and hardware for surveillance. A study of students at the University of New Hampshire found that approximately 10 - 15% of surveyed students reported receiving threatening or harassing email or Instant Messages (Finn, 2004).

Computer Monitoring Software. Computer Monitoring Software, or "SpyWare", was originally developed to monitor children's Internet use, but has also been utilized by abusers. It allows an abuser to monitor computer and Internet activities and discover a victim's efforts to escape or access help. This software can be installed remotely or by physically accessing the victim's computer. Although SpyWare detection programs claim to uncover the hidden SpyWare programs, they are imperfect in their counter surveillance. "Scrubber"

moment avec leur partenaire. Les agresseurs peuvent utiliser les nouveaux services de télécommerce mobile qu'offrent les entreprises de téléphonie cellulaire pour localiser leur victime. Au Rhode Island, un homme a agressé sa femme après avoir trouvé le numéro de téléphone du refuge où elle habitait dans l'historique de son téléphone cellulaire. Du coup, la femme a dû attendre un an avant de pouvoir quitter à nouveau son mari (Safety Net, 2004).

Appareils de localisation et de surveillance

Les traqueurs utilisent de plus en plus des technologies de localisation et d'imagerie, de base et sophistiquées, pour surveiller leurs victimes, ce qui rend ces dernières encore plus vulnérables. Avant que les agresseurs aient accès à des dispositifs de repérage comme le système mondial de localisation, ils vérifiaient souvent les compteurs kilométriques des voitures de leurs victimes pour surveiller leurs activités quotidiennes. Maintenant, ces agresseurs utilisent divers instruments, d'appareils photos numériques bon marché aux vidéo-caméras en continu et aux systèmes mondiaux de localisation de haute technologie qui, sans avoir été conçus pour la surveillance, servent à cette fin aux agresseurs.

Systèmes mondiaux de localisation. Pour localiser et suivre leurs victimes, les agresseurs se servent de systèmes mondiaux de localisation (GPS) reliés à des récepteurs de signaux de satellite qui peuvent fournir un positionnement précis en temps réel dans le monde entier. Ces appareils de tailles et d'aspects variés sont proposés à divers prix. Un GPS peut ressembler à une petite boîte noire ou à un portable, ou même prendre la forme d'une petite puce intégrée dans un serre-poignet. La technologie de positionnement mondial fait aussi partie des anti-vols pour véhicules comme OnStar. En décembre 2002, un résident du Wisconsin avait installé, à l'insu de son ex-petite amie, un appareil GPS sous le capot de sa voiture. Il l'a traquée ensuite pendant des mois. [traduction] « Il la suivait lorsqu'elle se rendait au travail ou faisait des courses. Il surgissait inexplicablement près de sa voiture à des feux de circulation et a même essayé une fois de la faire sortir de la route. » (Orland, 2003, par. 2). Comme les GPS sont de moins en moins chers, il est impératif que les survivantes reçoivent la formation nécessaire

and "Washer" programs that claim to clear computer histories are ineffective if SpyWare is in use. Additionally, if the victim installs new programs or clears all computer trails, this could cause suspicion and increase danger. In September 2001, a Michigan man was charged with installing spy software on the computer of his estranged wife. Without her knowledge, a SpyWare program sent him regular emails reporting all of her computer activity, including all emails sent and received and all web sites visited (Wendland, 2001).

Keystroke Logging Hardware. In addition to software programs, stalkers can use hardware devices called "Keystroke Loggers" that are inserted between the keyboard cable and the back of the computer. These tiny devices contain small hard drives that record every key typed, including all passwords, personal identification numbers (PIN), websites, and email. Abusers with physical access to a victim's computer can install and check these hidden devices. SpyWare software detection programs cannot detect hardware loggers. Both SpyWare software and keystroke logging hardware are advertised as products allowing one to easily "spy on your spouse."

Email & Instant Messages. Abusers are using email and instant messages to threaten victims and impersonate them. Stalkers can send victims malicious SpyWare or viruses as email attachments. Abusers are monitoring email and impersonating victims by stealing passwords and viewing email via SpyWare. One abuser changed his wife's email password and sent threatening messages to himself from her email account. He then took the printed messages to the police and asked them to arrest her. Another abuser killed his wife after discovering that she was planning to flee. He learned of her escape plan in an email in her "deleted email folder". (SafetyNet, 2004).

Websites. Stalkers are setting up websites that threaten victims or encourage others to contact, harass, or harm the victim. Some abusers encourage others to stalk their victim by posting erroneous and harassing information on websites (e.g. that the stalker's ex-wife enjoys being raped). In one scenario, an abuser had his parental rights terminated when his child was a toddler.Years later he posted a very old family photograph and details about his then ten-year-old child. The mother and child were terrified to discover the presence and content of this website (Safety Net,

pour apprendre à détecter leur présence.

Caméras cachées. Les traqueurs utilisent de petites caméras cachées pour surveiller leurs victimes et se renseigner sur leurs habitudes. Ils se servent de l'information recueillie pour exercer leur pouvoir et un contrôle sur leurs victimes. De petites caméras sans fil à haute résolution peuvent être cachées dans des détecteurs de fumée, des lampes d'enfant, ou derrière un trou de la taille d'une épingle dans un mur. Elles peuvent même être activées à distance. En 2003, la cour suprême du New Jersey a déclaré que la vidéosurveillance que le défenseur avait effectuée de la chambre de son ex-conjointe constituait une preuve *prima facie* de traque et de harcèlement en vertu de la *New Jersey Domestic Violence Act* (Loi sur la violence conjugale du New Jersey) (H.E.S. c. J.C.S., 2003).

Ordinateurs et Internet

Les agresseurs continuent à trouver et à adapter de nouveaux logiciels et des outils informatiques afin de traquer et de harceler encore plus leurs victimes. Ils n'utilisent pas seulement des moyens de surveillance de faible technicité comme l'examen de l'historique de navigation sur Internet ou l'interception des courriels, mais aussi de plus en plus de matériel informatique et de logiciels espions ultra sophistiqués. Une étude réalisée auprès des étudiants de l'université du New Hampshire a révélé que de 10 à 15 % des étudiants sondés avaient déclaré avoir été menacés ou harcelés dans des courriels ou par des messages instantanés (Finn, 2004).

Logiciels de surveillance. Les logiciels de surveillance ou « logiciels espions » ont été mis au point à l'origine pour surveiller l'utilisation d'Internet par les enfants, mais leur usage a été détourné par les agresseurs. Ces logiciels leur permettent de surveiller l'ordinateur et les activités sur Internet de leurs victimes et de découvrir les démarches qu'elles entreprennent pour leur échapper ou chercher de l'aide. Ils peuvent être installés à distance ou directement sur l'ordinateur de la victime. Bien que les programmes de détection des logiciels espions prétendent pouvoir découvrir les programmes cachés SpyWare de niveau 5, leur contre-surveillance n'est pas parfaite. Les programmes Scrubber et Washer dont les manufacturiers affirment qu'ils effacent l'historique des ordinateurs sont inefficaces en

2004).

Online Databases and Information Brokers. Stalkers use free and fee-based websites to track private information about their victims. Information brokers are commercial entities that buy and sell data, and frequently acquire information from public records and retail databases. In addition to fee-based services, many free websites such as court databases, voter registration, and religious directories provide a wealth of private contact information that can be used to track survivors nationwide as they attempt to relocate. Many courts are beginning to publish both indexes of court records and the full documents and case files to the Internet, often without providing any notice to citizens or options for victims to restrict web-access. The Montgomery County, Pennsylvania Court went a step further, publishing the names and addresses of victims (and their children) who obtain protection orders on the Internet (Webster, 2003, December 1).

Advocacy Response: What Can Advocates Do?

Victims of abuse begin to plan for safety well before they reach out to advocates and other practitioners for assistance. It is vital that advocates continue to support the strategies survivors have been successfully using to help them navigate the abuse and stalking in their lives. Regardless of an advocate's own level of technological expertise, it is important that advocates work with survivors to plan for safety around technology and stalking. Although technology is changing rapidly and abusers are adept at misusing these new tools, advocates should remember that the motive for stalking is not affected by technological advancements. Abusers stalk in order to maintain power and control over a victim. Therefore, safety planning with survivors about technology methods used to stalk her may have a similar format to other non-technology related safety planning approaches and advocacy. (See appendixes for further resources and materials.)

Survivor Advocacy

Some survivors have found that disconnecting a telephone line or email account in an attempt to thwart a stalker results in the abuser escalating to a new method of control or access. Advocates can work with survivors to find ways to limit stalker

présence d'un logiciel espion. De plus, si la victime installe de nouveaux programmes ou nettoie toutes les traces laissées sur son ordinateur, elle peut susciter de la suspicion et se mettre encore plus en danger. En septembre 2001, un résidant du Michigan a été accusé d'avoir installé un logiciel espion dans l'ordinateur de son ex-conjointe. Sans qu'elle le sache, le logiciel espion envoyait régulièrement par courriel à l'ex-conjoint un compte-rendu de toutes ses activités à l'ordinateur, y compris les courriels envoyés et reçus et tous les sites Web visités (Wendland, 2001).

Matériel d'enregistrement de frappe. En plus des logiciels, les traqueurs peuvent utiliser des appareils appelés « enregistreurs de frappe » qui s'insèrent entre le câble du clavier et l'arrière de l'ordinateur. Ces appareils minuscules contiennent de petits disques durs qui enregistrent toutes les frappes du clavier, dont les mots de passe, les numéros d'identification personnels (NIP), les sites Web et les courriels. Les agresseurs qui ont accès à l'ordinateur de leur victime peuvent installer et vérifier ces appareils cachés. Les programmes de détection des logiciels espions ne peuvent pas les détecter. Les publicités utilisées pour vendre les logiciels espions et le matériel d'enregistrement de frappe suggèrent qu'avec ces produits, on peut « espionner » facilement son conjoint ou sa conjointe.

Courriels et messages instantanés. Les agresseurs se servent des courriels et des messages instantanés pour menacer leurs victimes et se faire passer pour elles. Ils peuvent envoyer à leurs victimes des logiciels espions ou des virus malveillants en pièces jointes. Ils surveillent le courrier électronique des victimes ou usurpent leur identité en volant leurs mots de passe ou en consultant leurs courriels au moyen d'un logiciel espion. Un agresseur a changé le mot de passe du courrier électronique de sa femme et s'est envoyé à lui-même des messages menaçants à partir du compte de sa femme. Il a ensuite apporté les messages imprimés à la police et leur a demandé de l'arrêter. Un autre agresseur a tué sa femme après avoir découvert qu'elle se préparait à s'enfuir. Il avait découvert son plan de fuite dans son dossier de courriels effacés (SafetyNet, 2004).

Sites Web. Les traqueurs créent des sites Web où ils menacent leurs victimes et encouragent d'autres personnes à communiquer avec elles, à

access, collect evidence, and maintain their safety. For example, some survivors have installed a new telephone line, but left the old telephone number connected with the ringer turned off. This allows them to document the continued harassing calls with an answering machine and caller ID. Advocates must work with victims to navigate these risks and weigh the potential safety risks of evidence collection. For example, law enforcement might interview the abuser or seize the stalker's computer. Advocates need to discuss with the victims the possible increased risks that law enforcement or criminal justice system involvement might create. Sometimes stalkers react violently when they find out that the victim has reported to the police or sought a protection order. These types of interventions are often necessary and life-saving, but victims need to know that stalkers are unpredictable and these interventions also may bring risk. Advocates need to safety plan with victims accordingly. Situations like these must be carefully analyzed to ensure that victim safety is not overlooked in an effort to hold offenders accountable.

Strategies for Advocates:

- Focus on the survivor's needs and make sure that the options suggested are feasible.
- Try to share information about technology safety risks in ways that are relevant to theconcerns raised by a survivor. Some survivors may feel relieved to finally figure out why their stalkers are able to know everything they do; others may choose to focus first on otherpriorities and prefer to discuss technology information later.
- Consider introducing the topic of technology stalking and safety in survivor support groups. Also educate victims about the positive benefits of emerging technology tools that can enhance their safety.
- Educate survivors about these new tools and the potential use of technology to stalk without prohibiting access to technology. For example, explain cell phone features to survivors, but do not ban cell phones from shelter. Advocates might also provide safer computer and Internet access and education to victims in shelter.
- Some survivors may have heightened risks of stalking through technology and may need additional information and support. For example, some people with disabilities rely on

les harceler ou à leur faire du mal. Certains agresseurs encouragent aussi d'autres à traquer leurs victimes en affichant sur des sites Web des informations fausses ou malveillantes (p. ex., que l'ex-conjointe du harceleur aime être violée). Dans une affaire, un agresseur avait perdu ses droits parentaux lorsque son enfant était tout petit. Des années après, il a affiché une très vieille photo de famille et des renseignements sur son enfant alors âgé de 10 ans. La mère et l'enfant ont été terrifiés par la découverte de ce site Web et de son contenu (Safety Net, 2004).

Banques de données et courtiers en information en ligne. Les traqueurs utilisent des sites Web gratuits ou payants pour rechercher des renseignements personnels sur leurs victimes. Les courtiers en information achètent et vendent des données et tirent fréquemment des renseignements de dossiers publics ou de banques de données de commerces de détail. En plus des services payants, de nombreux sites gratuits comme les banques de données des cours de justice, les fichiers d'électeurs et les répertoires des Églises fournissent une foule de renseignements personnels que les agresseurs peuvent utiliser pour traquer les survivantes dans tout le pays, alors que celles-ci essayent de déménager. Nombreuses sont les cours de justice qui commencent à publier leurs répertoires de dossiers, les documents complets ainsi que les dossiers judiciaires sur Internet, souvent sans même en avertir les parties intéressées ou offrir aux victimes la possibilité de restreindre l'accès sur Internet. La Montgomery County Pennsylvania Court a franchi un pas de plus en publiant les noms et adresses des victimes (et de leurs enfants) qui avaient obtenu des ordonnances de protection sur Internet (Webster, 1er décembre 2003).

Réponse des groupes de défense : que peuvent-ils faire?

Les victimes d'abus commencent à planifier leur sûreté bien avant de demander l'aide des groupes de défense ou d'autres intervenants. Il est essentiel que ces derniers continuent de soutenir les stratégies employées avec succès par les survivantes pour vivre avec les abus et la traque dont elles font l'objet, et que, peu importe leur propre degré de familiarisation avec la technologie, ils aident les survivantes à planifier leur sûreté lorsqu'ils utilisent la technologie ou ont

assistive technologies to communicate and access resources online and might be more vulnerable to specific methods of technology monitoring and stalking. Consider additional factors — such as geographic location, ethnicity, income, accessibility, age, or sexual orientation — that could impact a survivor's access to or reliance on various communications or technology.

- Educate survivors about the timing challenges of some digital evidence such as voicemail messages, telephone traces, Internet user records, and email "headers." If a victim wants to report these crimes to the police, law enforcement may have a short window to collect the digital evidence since many companies only retain the information for a very limited amount of time. For example, some Internet service providers only keep user records for thirty days.

Technology and Organizational Change

There are many critical action steps advocates can implement within their organizations to improve the response to victims and increase survivor safety regarding technology. First, advocates can educate and train all staff and volunteers about both the positive benefits of technology and also how abusers are misusing technology to stalk their partners. Next, advocates should examine if high-tech stalkers could compromise any of their own organizational practices.

Many nonprofit organizations and government agencies are embracing technology without a thorough understanding of potential unintended consequences. As data systems become increasingly interconnected, it is vital that advocacy organizations anticipate and minimize the potential for harm to survivors, by securing the confidentiality of all communications, and reexamining and minimizing any data about survivors that is collected, stored, and shared. Additionally, since some victims will request online assistance or advocacy, it is critical for advocates to think proactively through all safety, confidentiality, stalking, and monitoring possibilities, and, to create survivor-centered organizational practices that increase confidentiality, informed consent, and safety planning (Finn, 2001; Kranz, 2001).

affaire à un traqueur. Bien que la technologie évolue rapidement et que les agresseurs aient maîtrisé l'art d'utiliser ces nouveaux outils à mauvais escient, les groupes de défense ne doivent pas oublier que les motifs d'un traqueur ne sont pas influencés par les percées technologiques. Un agresseur traque une victime dans le but de maintenir son emprise sur elle. Donc, la planification de la sûreté de concert avec les survivantes pour les prémunir contre les moyens techniques employés par les traqueurs prend parfois une forme semblable à d'autres méthodes de planification de la sûreté et à d'autres activités de défense n'ayant rien à voir avec la technologie. (Voir les annexes pour d'autres ressources et documents.)

Défense des intérêts des survivantes

Certaines survivantes ont constaté qu'en débranchant leur ligne téléphonique ou en fermant leur compte de courrier électronique dans le but de contrecarrer les efforts du traqueur, elles n'avaient que poussé ce dernier à trouver un nouveau moyen d'exercer son emprise sur elles ou un nouveau chemin d'accès. Les groupes de défense peuvent aider les survivantes à trouver des façons de limiter l'accès d'un traqueur, de recueillir des éléments de preuve et de garantir leur sûreté. Ainsi, certaines survivantes ont installé une nouvelle ligne téléphonique et laissé l'ancienne branchée mais en coupant la sonnerie du téléphone. Cela leur a permis d'utiliser un répondeur et l'afficheur pour garder une trace de tous les appels importuns. Les groupes de défense doivent apprendre aux victimes à vivre avec cette réalité et à peser les risques éventuels que pose la collecte d'éléments de preuve pour leur sécurité, car cela peut amener les policiers, par exemple, à interroger le traqueur ou à saisir son ordinateur. Ils doivent discuter avec les victimes du fait que l'entrée en jeu des policiers ou de l'appareil de justice pénale peut les exposer à un risque accru. En effet, il arrive que des traqueurs réagissent avec violence lorsqu'ils constatent que la victime les a dénoncés à la police ou s'est prémunie d'une ordonnance de protection. Ces types d'interventions sont souvent nécessaires et peuvent sauver une vie, mais les victimes doivent savoir que les traqueurs sont des gens imprévisibles et que ces interventions s'accompagnent d'un certain risque. Les groupes de défense doivent donc planifier la sécurité des victimes en conséquence. Ces situations doivent être soigneusement analysées pour éviter que la

Strategies for Advocates:

- Revise organizational communication, records, and confidentiality policies to include technology security issues.
- Update organization website safety information for victims searching for support online. Also, ensure that your website is accessible to all survivors, including individuals with disabilities who use assistive technology such as screen readers.
- Create organizational policies that address how (or if) to respond to emails from victims. When reviewing policies, consider the possibility that abusers may be monitoring the victim's email account or computer, so policies should focus on how to increase safety and always provide informed consent.
- Increase victim safety by securing survivor data. Only store victim information on computers that are not connected to the Internet or networked to the Internet. If using an Internet-based database for victim records, designate a computer to use only for that purpose.To minimize hacking and SpyWare risks, do not store other victim files on that computer or use it for email or Internet browsing.
- Given that abusers work in every field and some are extremely skilled in using technology, evaluate data collection and sharing policies to keep victim data out of the hands of stalkers, abusers, and members of the public.

Technology & Legal Advocacy

As stalkers increase their use of technology, it is vital that communities are equipped to respond to these crimes. In an age where stalkers can easily use search engines to track them, victims need to be able to relocate safely. As more records are published to the Internet, advocates must educate community agencies, courts, and government offices about the potential dangers to victims and the importance of notification and privacy options. When electronic evidence is needed to prosecute a crime, advocates can work to ensure that specialized violence against women law enforcement and prosecution units receive additional training or access to a technology crime unit. Whether working within the legal system, community social services, or with other civic organizations, education and systems advocacy are critical to lessening the barriers victims of

sûreté des victimes ne soit oubliée dans les efforts déployés pour tenir les contrevenants responsables de leurs actes.

Stratégies pour les groupes de défense

- Concentrez-vous sur les besoins de la survivante et assurez-vous que les options proposées soient faisables.
- Essayez de transmettre l'information sur les risques liés à la sécurité de la technologie d'une manière qui reflète les préoccupations soulevées par la survivante. Certaines survivantes se sentent parfois soulagées de comprendre enfin comment un traqueur est capable de connaître leurs moindres faits et gestes, alors que d'autres préféreront mettre d'abord l'accent sur d'autres priorités et discuter de la technologie ultérieurement.
- Songez à aborder les thèmes de l'utilisation de la technologie aux fins de traque et de la sécurité dans le cadre de groupes de soutien aux survivantes. Renseignez aussi les victimes sur les avantages des nouveaux outils technologiques susceptibles d'accroître leur sécurité.
- Familiarisez les survivantes avec ces nouveaux outils et expliquez-leur que la technologie peut être utilisée pour traquer quelqu'un sans qu'on ne soit obligé pour autant d'en interdire l'accès. Par exemple, parlez-leur des fonctions des cellulaires, mais n'interdisez pas ces appareils dans les refuges. Les groupes de défense peuvent également offrir un accès mieux sécurisé à un ordinateur et à Internet, et des séances de sensibilisation à cet effet, dans les refuges.
- Certaines survivantes sont plus exposées que d'autres au harcèlement à l'aide de moyens techniques et pourraient avoir besoin de renseignements et d'un soutien supplémentaires. Par exemple, certaines personnes handicapées doivent recourir aux technologies d'assistance pour communiquer et accéder aux ressources en direct; elles risquent donc d'être plus vulnérables à certaines méthodes de surveillance et de traque fondées sur la technologie. Rappelez-vous que certains facteurs additionnels, comme l'emplacement géographique, l'origine ethnique, le revenu, l'accessibilité, l'âge ou l'orientation sexuelle peuvent avoir une incidence sur l'accès d'une survivante à divers modes de communication ou à diverses technologies, ou sur l'utilisation

technology stalking encounter.

Strategies for Advocates:

- Identify training opportunities on technology investigation, computer forensics, or prosecution, and attend these trainings with law enforcement or prosecutors from your community. Many states have computer crime units or prosecutor associations that may be available to support and train local jurisdictions.
- Identify the police and prosecutor technology crime specialists. If the community does not have a technology unit, identify officers and prosecutors with technology experience. Discuss how law enforcement process digital evidence and conduct investigations.
- Work with law enforcement to identify what evidence is needed, so advocates can work with survivors to document the necessary information. Encourage officers and survivors to discuss how the investigation will impact the victim's life. For example, if a victim's computer is seized, it may be possible to duplicate the hard-drive and return it quickly.
- Work with the legal system to identify the state laws that could apply to emerging technology strategies of stalkers. Some stalking laws only include electronic communication devices, so prosecutors may need to use eavesdropping or other statutes to address some crimes.
- Ask that prosecutors discuss the potential consequences with a survivor of pursuing a technology related criminal charge compared to a domestic violence or stalking charge, so that she remains informed of how potential media coverage and evidence collection practices might impact her life. For example, national and international media covered the Michigan SpyWare and the Wisconsin GPS stalking cases.
- Join community committees discussing Internet publication of court or voter records and advocate for privacy provisions for survivors.

Conclusion

While much is unknown about the future of technology and the emerging uses of technology in intimate partner stalking, advocates and allies must continue to press on - learning, educating, and advocating for change. Stalkers are persistent and resourceful, but so are the advocates and

qu'elle en fait.

- Sensibilisez les survivantes à l'importance du facteur temps lié à certains éléments de preuve numériques comme les messages sur boîte vocale, les appels téléphoniques dépistés, les archives sur l'utilisation d'Internet et les en‑têtes de messages électroniques. Si une victime souhaite signaler un crime, les policiers risquent de n'avoir que peu de temps pour recueillir les éléments de preuve numériques, car de nombreuses entreprises ne conservent l'information pertinente que pendant une durée limitée. Ainsi, certains fournisseurs Internet gardent les archives des utilisateurs durant trente jours seulement.

Technologie et changement organisationnel

Il existe de nombreuses mesures importantes que les groupes de défense peuvent mettre en œuvre pour mieux répondre aux besoins des victimes et accroître la sécurité des survivantes par rapport à la technologie. Premièrement, ils peuvent sensibiliser et former tout le personnel et les bénévoles concernant, d'une part, les avantages de la technologie et, d'autre part, la manière dont les traqueurs s'en servent à l'endroit de leurs partenaires. Deuxièmement, ils devraient déterminer si les traqueurs qui se servent de la haute technologie risquent de compromettre leurs propres pratiques organisationnelles.

Bon nombre d'organisations à but non lucratif et d'organismes gouvernementaux accueillent à bras ouvert la technologie sans toutefois connaître à fond les conséquences involontaires qu'elle pourrait entraîner. Les systèmes de données étant de plus en plus étroitement liés entre eux, il est crucial que les organismes de défense anticipent et minimisent le potentiel de danger pour les survivantes en garantissant la confidentialité de toutes les communications, ainsi qu'en réexaminant et en limitant les données sur les survivantes recueillies, stockées et partagées. De plus, étant donné que certaines victimes demanderont une aide ou une intervention en ligne, il est important que les groupes réfléchissent dans une optique prévoyante à toutes les possibilités qui pourraient survenir en matière de sécurité, de confidentialité, de harcèlement et de surveillance, et élaborent des pratiques organisationnelles axées sur la survivante qui renforcent la confidentialité, le consentement éclairé et la planification de la sûreté (Finn, 2001; Kranz, 2001).

survivors working against them.

Advocates should educate survivors and colleagues about emerging stalking methods, expand safety planning to include technology, and work with their local community systems to address the use of technology in intimate partner stalking. While it is imperative to immediately begin addressing technology issues, it is also important to realize that as technology continues to develop and abusers adapt to these changes, the response of advocates must change as well.

Anecdotal and empirical evidence clearly indicate that traditional modes of stalking have expanded, but significant research is needed to fully understand the parameters and types of technology used in stalking. Research is also needed to document the myriad of ways in which victims are creatively using technology to enhance their safety. More thorough study and documentation of use of technology by intimate partner stalkers is needed to expand our understanding of what survivors are experiencing and to inform the systemic change needed to address this issue. In the interim, advocates and allies are vital resources in providing critical support and helping victims plan for safety.

Appendix A: Technology Safety Planning - Tips for Advocates

This checklist of tips for advocates is intended to accompany the attached paper.

Telephones:

- Talk to survivors about screening calls with answering machines and, where legal, taping harassing telephone calls.
- Encourage victims to document harassing calls through stalking logs, photographing caller ID, and "call trace" (*57 in most areas).
- Educate survivors about "per-call" (*67 in most areas) or permanent caller ID blocking.
- Inform victims that caller ID devices can be installed without their knowledge and transmit information about all incoming calls.
- When calling victims, use caller ID Block or operator-assisted calls to reduce the risk of an abuser identifying an advocacy organization through a caller ID device.
- Call ahead before sending any faxes on behalf of a survivor. Encourage victims to do the same when they are not in shelter.

Stratégies pour les groupes de défense

- Révisez les politiques organisationnelles en matière de communication, d'archivage et de confidentialité afin d'inclure des dispositions sur la sécurité des technologies.
- Sur le site Internet de l'organisation, mettez à jour l'information sur la sécurité destinée aux victimes à la recherche de soutien en ligne. De plus, assurez-vous que votre site est accessible à toutes les survivantes, y compris les personnes handicapées qui utilisent des technologiques d'assistance comme des lecteurs écrans.
- Élaborez des politiques organisationnelles qui expliquent, s'il y a lieu, comment répondre aux messages électroniques des victimes. Lorsque vous révisez les politiques, dites-vous qu'il se peut que le traqueur surveille le compte de courrier électronique ou l'ordinateur de la victime. Les politiques devraient donc insister sur la manière d'accroître la sécurité et de toujours favoriser un consentement éclairé.
- Renforcez la sécurité de la victime en protégeant les données sur les survivantes. Ne sauvegardez l'information sur les victimes que dans des ordinateurs qui ne sont pas branchés, notamment par réseau, à Internet. Si vous tenez des dossiers sur les victimes dans une base de données reliée à Internet, réservez un ordinateur à cette fin uniquement. Afin de limiter le plus possible les risques de piratage ou d'espionnage informatique, ne stockez aucun autre dossier se rapportant aux victimes sur ce même ordinateur. N'utilisez pas non plus cet ordinateur pour le courrier électronique ou la navigation Internet.
- Étant donné qu'on trouve des agresseurs dans différents domaines d'activité, certains sont extrêmement versés dans l'utilisation de la technologie; évaluez les politiques de collecte et de partage des données de manière à garder les données sur les victimes hors de portée des traqueurs, des agresseurs et du grand public.

Technologie et parrainage juridique

Face à l'engouement des traqueurs pour la technologie, la société doit impérativement se doter de moyens pour mettre en échec cette forme de criminalité. De nos jours, comme les traqueurs peuvent facilement utiliser des moteurs de recherche pour traquer leurs victimes, celles-ci doivent être en mesure de changer de domicile en

Remind the fax recipient to cut off the fax header and remove cover page.

- Block caller ID on shelter and advocacy organization fax and telephone lines.
- Encourage victims to use a password or phrase when using communicating by TTY to confirm their identity and minimize the risk of impersonation.
- Talk with victims about deleting TTY conversation histories stored in their TTY devices.
- Provide a TTY device in advocacy offices that victims can use to make private calls.
- Encourage survivors to contact their telephone carriers to learn about their wireless/cell phone's features and services.They may want to ask if location services have been added to their service plans.
- Educate survivors about the option of turning a phone off to increase location privacy. Educate and strategize, but do not prohibit the use of cell phones in shelters or advocacy offices.
- Encourage survivors to use a donated cell phone or to purchase a new cell phone with a different carrier if they think their phones or the billing records are being used to monitor their calls.

Location and Surveillance:

- Encourage victims to trust their instincts if they suspect they are being followed.
- Help survivors find a law enforcement officer or a mechanic willing to search a victim's car or belongings for a GPS device.
- Talk to victims who use GPS automobile services about the pros and cons of changing their account password to prevent stalkers from gaining access to their car and location information.
- Encourage survivors to trust their instincts and look for patterns in the information the stalker appears to know. Patterns may help the survivor identify possible camera locations.
- Talk to survivors about checking their homes or having law enforcement search for small holes or unidentifiable wiring.

Computers:

- Encourage victims to use a safer computer; one that the stalker does not have access to.
- Encourage survivors not to open any attachments from unknown sources or their

toute sûreté. De plus en plus de documents sont publiés sur Internet, et c'est pourquoi les groupes de défense doivent sensibiliser les organismes locaux, les tribunaux et les pouvoirs publics aux dangers potentiels pour les victimes et à l'importance d'émettre des avis et d'offrir des options avant de divulguer des renseignements personnels. Quand il faut produire des éléments de preuve électroniques pour inculper un traqueur, les groupes de défense peuvent faire en sorte que les forces policières et les procureurs spécialisés dans la répression de la violence contre les femmes reçoivent une formation poussée ou aient accès à une unité de la criminalité technologique. Que les activités de plaidoyer soient entreprises au sein de la filière juridique, des services sociaux communautaires ou d'autres organismes civils, la sensibilisation et la défense des intérêts sont cruciales pour réduire les barrières auxquelles se heurtent les victimes de la traque technologique.

Stratégies pour les groupes de défense

- Soyez à l'affût des occasions de formation en matière d'enquêtes technologiques, d'informatique judiciaire ou de poursuites, et prenez-y part aux côtés de représentants des forces de l'ordre et de procureurs de votre communauté. De nombreux États ont des unités de la criminalité informatique ou des associations de procureurs qui pourraient vous aider à former les pouvoirs locaux.
- Dressez une liste de spécialistes de la criminalité technologique parmi les forces policières et les procureurs. Si vous n'avez pas d'unité technologique dans votre région, trouvez des policiers ou des procureurs qui ont de l'expérience en technologie, et discutez avec eux de la façon de traiter des éléments de preuve numériques et de mener des enquêtes.
- Travaillez avec les autorités compétentes à recenser les éléments de preuve nécessaires, de sorte que les groupes de défense puissent aider les survivantes à consigner par écrit les informations nécessaires. Encouragez les policiers et les survivantes à échanger sur la façon dont l'enquête peut affecter la vie de la victime. Si on doit réquisitionner l'ordinateur de la victime, par exemple, il est possible dans une telle éventualité de faire une copie de son disque dur et de lui rendre son ordinateur rapidement.
- Collaborez avec les autorités judiciaires à

abusers, and to keep their computers' operating systems and virus definitions updated regularly.
- Ask victims if they use a computer and, if so, explain how SpyWare can give an abuser the ability to monitor ALL computer use. Discuss the pros and cons of using SpyWare detection programs, since installing such a software program could alert the stalker.
- Encourage survivors to be suspicious if an abuser has installed a new keyboard recently or done computer repair work that coincides with an increase of stalking or monitoring.
- If a victim finds a harassing website about herself, discuss with her the option of talking to law enforcement to determine whether a website is a violation of a protection order or could be evidence for a stalking or harassment charge.
- Help victims use search engines such as www.whois.net to determine the owner of a malicious website and research the website owner's policy on threatening sites.
- Encourage victims to ask where their personal information is stored; if any government entities publish their records on the Internet, they can request to have their records sealed or to restrict who can access their information.
- Identify or promote approaches, such as address confidentiality programs, which provide viable mechanisms to ensure a victim's information remains confidential regardless of whether she votes, buys property, goes to court, or engages in other activities.

Appendix B: Annotated Resource Lists For Advocates

This list highlights select technical assistance projects, websites, and written materials chosen for practical usefulness to advocates who are working with survivors of technology-based intimate partner stalking.

A. U.S.Technical Assistance Projects

The Safety Net Project at the National Network to End Domestic Violence Fund
660 Pennsylvania Ave SE, Suite 303;Washington, DC 20003
Phone: 202-543-5566 x 22
Fax: 202-543-5626
Email: safetynet@nnedv.org

recenser les lois de l'État qui pourraient s'appliquer à des stratégies technologiques de traque nouvelles. Certaines lois réprimant la traque s'appliquent uniquement aux dispositifs de communication électroniques et, donc, les procureurs pourraient avoir à faire de l'écoute ou à invoquer d'autres textes réglementaires pour sévir contre certains crimes.
- Demandez aux procureurs de parler à une survivante des conséquences possibles d'une poursuite pour crime technologique par opposition à une inculpation pour violence familiale ou traque pour qu'elle soit consciente des répercussions de la couverture médiatique possible et des pratiques de collecte des éléments de preuve sur sa vie. Citez par exemple la couverture par les médias nationaux et internationaux des procès pour traque Michigan SpyWare et Wisconsin GPS.
- Joignez-vous à des comités locaux s'intéressant à la publication sur Internet des délibérations des tribunaux et des listes électorales, et plaidez en faveur de dispositions légales pour protéger la vie privée des survivantes.

Conclusion

Bien que l'on ignore encore beaucoup de choses sur l'avenir de la technologie et des usages futurs de celle-ci pour la traque d'un partenaire intime, les groupes de défense des victimes de traque et leurs alliés doivent néanmoins continuer de militer en faveur du changement en poursuivant leur apprentissage et leurs activités de sensibilisation. Certes les traqueurs sont tenaces et astucieux, mais leurs victimes et les groupes qui travaillent à les mettre en échec le sont aussi.

Les groupes de défense devraient sensibiliser les survivantes et leurs collaborateurs aux nouvelles méthodes de traque, étendre la planification des mesures de sûreté à la technologie et travailler avec les organismes locaux à maîtriser l'utilisation de la technologie dans la traque des partenaires intimes. Même si les enjeux de la technologie exigent une action immédiate, il est tout aussi important de se rappeler que la technologie évolue constamment et que les agresseurs s'y adaptent. Il faut donc que les défenseurs aussi ajustent leur tir.

Les informations empiriques indiquent clairement

http://www.nnedvfund.org
Description: Launched in August 2002, Safety Net: the National Safe &Strategic Technology Project at the National Network to End Domestic Violence Fund (NNEDV) addresses all forms of technology that benefit survivors, are misused by abusers, or impact survivors in their communities. The Safety Net Project provides training and technical assistance to U.S. state domestic violence coalitions, local advocates, law enforcement, prosecutors, and allies on all forms of technology that impact victims of abuse.

The Stalking Resource Center at the National Center for Victims of Crime
2000 M Street NW, Suite 480, Washington, D.C. 20036
TTY: 1-800-211-7996
Phone: 1-800-FYI-CALL (1-800-394-2255)
Fax: 202-467-8701
http://www.ncvc.org/src
Description: The Stalking Resource Center is a program of the National Center for Victims of Crime. Launched in July 2000 with funding from the Office on Violence Against Women, their dual mission is to raise national awareness of stalking and to encourage the development and implementation of multidisciplinary responses to stalking in local communities across the U.S. The Stalking Resource Center provides training and technical assistance on all forms of stalking (including high technology stalking) and community response. The Stalking Resource Center maintains a website with articles, news stories, stalking legislation and case law, and many more resources for practitioners and victims. In addition, they produce two newsletters per year and have brochures that can be downloaded from their website.

The National Domestic Violence Hotline /Linea Nacional sobre la Violencia Domestica
PO Box 161810, Austin, TX 78716
TTY 1-800-787-3224
Phone: 1-800-799-SAFE (7233)
http://www.ndvh.org
Description: This toll free hotline enables victims of domestic violence, their families, advocates, and friends to call trained hotline advocates/ counselors who will provide confidential crisis intervention, support, information and referrals to local programs. The hotline links people to shelters, and legal and social assistance programs in their geographic area. Advocates provide help in English and Spanish with

que les modes de traque traditionnels ont évolué, mais il reste qu'il faudrait entreprendre des recherches approfondies pour comprendre pleinement les paramètres et les types de technologies utilisés par les traqueurs. Il faudrait également recenser la multitude de façons dont les victimes se servent judicieusement de la technologie pour accroître leur sûreté. Enfin, il faudrait étudier et étayer davantage l'utilisation de la technologie dans la traque d'un partenaire intime avant de pouvoir comprendre ce que vivent les survivantes et proposer les changements systémiques qui s'imposent. D'ici là, les groupes de défense et leurs alliés demeureront des ressources vitales dans la prestation d'un soutien essentiel et d'une aide aux victimes dans la planification de la sûreté.

Annexe A : Planification de la sûreté des technologies – Conseils à l'intention des groupes de défense

La liste ci-dessous de conseils à l'intention des groupes de défense se veut un complément au présent rapport.

Téléphones

- Proposez aux survivantes de filtrer leurs appels à l'aide d'un répondeur et, lorsque la loi le permet, d'enregistrer les appels importuns.
- Encouragez les victimes à prendre des notes sur les appels importuns, par exemple en tenant un registre des appels, en photographiant le numéro affiché et en utilisant le service Dépisteur (*57 dans la plupart des régions).
- Renseignez les survivantes au sujet du service de blocage permanent de l'affichage (*67 dans la plupart des régions).
- Informez les victimes que des dispositifs d'affichage des appels peuvent être installés à leur insu et transmettre de l'information sur tous les appels qu'elles reçoivent.
- Lorsque vous appelez une victime, activez la fonction de blocage de l'affichage ou faites acheminer l'appel par un téléphoniste afin d'atténuer le risque qu'un agresseur identifie votre groupe de défense à l'aide de son dispositif d'affichage.
- Avant d'envoyer un document par télécopie de la part d'une survivante, appelez avant. Incitez les victimes à faire de même lorsqu'elles ne se trouvent pas dans un

interpreters available for 139 languages. Crisis intervention and referrals are available to the Deaf through a TTY line or by email to deafhelp@ndvh.org Call the hotline 24 hours a day from anywhere in the U.S.

<u>B.Websites on Responding to Technology Use in Intimate Partner Stalking</u>

The Privacy Rights Clearinghouse
http://www.privacyrights.org
Description: The Privacy Rights Clearinghouse is a nonprofit consumer education, research, and advocacy program. While PRC's information is written for the general public and does not specifically focus on intimate partner stalking, advocates can find many fact sheets, speeches, and articles with overviews and practical tips for survivors on internet privacy, various telephone and telecommunications issues, public and government records, and more.

Stalking Resource Center - Stalking Laws &Court Cases collections
Stalking Laws: http://www.ncvc.org/src/main.aspx?dbID=DB_All_Legislation188
Stalking Court Cases: http://www.ncvc.org/src/main.aspx?dbID=DB_All_Case_Law508
Description: These web-based collections present laws and court case summaries for various U.S. jurisdictions: federal, federal interstate, state, and Tribal. These are useful for educating advocates and survivors about laws that can be used to hold an abuser accountable for using technology to stalk. The text of stalking laws and related legal offenses such as: harassment by telephone, cyberstalking, and unlawful computerized communications are covered in the stalking laws state-by-state section. The stalking court cases section summarizes federal and state court case findings, including where using technology to stalk an intimate partner was found by law to be a crime.

SafetyEd International
http://www.safetyed.org
Description: Housed in New Zealand, this website provides education regarding online safety and privacy. It includes research articles, online workshops, U.S. legal summaries, and other advocacy articles on cyberstalking.

Working to Halt Online Abuse (WHOA)
http://www.haltabuse.org
Description: WHOA fights "online harassment

refuge. Rappelez au récipiendaire de supprimer l'en-tête et d'enlever la page couverture.

- Bloquez l'affichage pour les communications faites par téléphone et par télécopieur à partir du refuge et des bureaux du groupe de défense.
- Encouragez les victimes à confirmer leur identité par un mot de passe ou une phrase-clé lorsqu'elles communiquent par téléimprimeur (TTY), afin de limiter le risque d'usurpation d'identité.
- Discutez avec les victimes de la possibilité de supprimer les conversations emmagasinées dans leur TTY.
- Installez dans les bureaux de votre groupe de défense un TTY que les victimes pourront utiliser pour communiquer en privé.
- Invitez les survivantes à appeler leur compagnie de téléphone afin de se renseigner sur les fonctions et les services de leur appareil sans fil/cellulaire. Elles pourraient notamment demander si des services de localisation ont été ajoutés à leur plan de services.
- Dites aux survivantes qu'elles ont toujours la possibilité de débrancher leur téléphone afin de mieux protéger la confidentialité de l'endroit où elles se trouvent. Faites de la sensibilisation et élaborez des stratégies, mais n'interdisez pas l'utilisation des cellulaires dans les refuges ou les bureaux de votre groupe de défense.
- Encouragez les survivantes à se servir d'un cellulaire donné ou à acheter un nouveau cellulaire auprès d'une entreprise de télécommunications différente si elles craignent que quelqu'un utilise leur téléphone ou leurs factures pour surveiller leurs appels.

Localisation et surveillance

- Incitez les victimes à faire confiance à leur instinct si elles se croient traquées.
- Aidez les survivantes à trouver un policier ou un mécanicien prêt à passer leur voiture et leurs effets personnels au peigne fin pour trouver un éventuel système mondial de localisation (GPS).
- Discutez avec les victimes qui utilisent un GPS dans leur voiture des avantages et des inconvénients qu'il y a à changer leur mot de passe afin d'empêcher les traqueurs d'avoir accès à leur véhicule et de connaître leur emplacement.
- Encouragez les survivantes à faire confiance

through education of the general public, education of law enforcement personnel, and empowerment of victims". WHOA's website provides links to various resources regarding online harassment and stalking, and suggests some tips to increase safety. WHOA responds to a range of issues faced by survivors of stranger and acquaintance stalking, many of which can also be relevant to intimate partner stalking.

C. Written Materials on Responding to Technology Use in Intimate Partner Stalking

Address Confidentiality Programs
Author: Vote Power Project, NNEDV Fund (2004)
Description: This document lists U.S. states with address confidentiality programs, and provides telephone numbers and web-based access to relevant state forms, qualifying information, and process steps.
http://www.nnedvfund.org/default.asp?Page=63

Annotated Stalking Bibliography
Author: Stalking Resource Center, National Center for Victims of Crime (NCVC)
Description: This bibliography provides brief summaries of over thirty materials on stalking, all published after 1994.The bibliography notes when the article addresses intimate partner stalking or cyberstalking.
http://www.ncvc.org/src/main.aspx?dbID=DB_Annotated_Stalking_Bibliography344

Data Security Checklist to Increase Victim Safety &Privacy
Author: Safety Net: the National Safe &Strategic Technology Project, the National Network to End Domestic Violence Fund (Safety Net, NNEDV) (2004)
Description: This handout provides steps to consider when undertaking such activities as designing a data collection system or securing a local organization's network. These tips help ensure victim-related data will be better protected and remain confidential from high-tech stalkers and hackers.
http://www.nnedvfund.org/pdf/NNEDVDataSecurity.pdf

Domestic Violence Organizations Online: Risks, Ethical Dilemmas, and Liability Issues
Author: Jerry Finn (2001)
Description: This paper outlines risk and liability considerations related to the use of the Internet for advocates working with survivors of stalking and

à leur instinct et à essayer de dégager des tendances dans l'information que le traqueur semble avoir en sa possession. Ces tendances pourraient les aider à trouver l'emplacement d'éventuelles caméras.

- Recommandez aux survivantes de passer leur logement au peigne fin, ou de demander à un policier de le faire, afin de repérer toute petite ouverture pratiquée ou tout fil non identifiable.

Ordinateurs

- Encouragez les victimes à utiliser un ordinateur à moindre risque, auquel le traqueur ne peut avoir accès.
- Dites aux survivantes de ne pas ouvrir les pièces jointes de source inconnue ou envoyées par leur agresseur, et de mettre à jour régulièrement le système d'exploitation et l'antivirus de leur ordinateur.
- Demandez aux victimes si elles utilisent un ordinateur et, le cas échéant, expliquez-leur comment les logiciels espions peuvent permettre à un agresseur de surveiller toutes les utilisations qu'elles font de leur ordinateur. Discutez avec elles des avantages et des inconvénients que présentent les programmes de détection de ce genre de logiciels, car leur installation pourrait alerter le traqueur.
- Encouragez les survivantes à faire preuve de vigilance si un agresseur a installé un nouveau clavier dernièrement ou fait des réparations à l'ordinateur qui coïncident avec une intensification de la traque ou de la surveillance.
- Si une victime trouve un site Internet harcelant à son endroit, parlez-lui de la possibilité de contacter les autorités compétentes afin de déterminer si le site contrevient à une ordonnance de protection ou pourrait servir de preuve pour une accusation de traque, voire de harcèlement criminel.
- Aidez les victimes à utiliser les moteurs de recherche comme www.whois.net, afin de trouver le propriétaire d'un site malveillant et de prendre connaissance de sa politique sur les sites où sont proférées des menaces.
- Incitez les victimes à demander où sont stockés leurs renseignements personnels; si un organe gouvernemental publie leurs dossiers sur Internet, elles peuvent demander que ces derniers soient scellés ou qu'on en restreigne l'accès.
- Trouvez ou favorisez des outils comme les programmes de protection de la confidentialité des adresses, qui offrent des mécanismes

domestic violence. It discusses potential safety, privacy, and security risks for survivors communicating and accessing direct services online.
http://www.vaw.umn.edu/documents/commissioned/online_liability/online_liability.html

Helpful or Harmful? How Innovative Communication Technology Affects Survivors of Intimate Violence
Author: Ann L. Kranz (2001)
Description: This paper explores web usage by both survivors of intimate violence and the organizations that serve them. It highlights ways that batterers use communication technology to monitor and control their partner's activities, and notes safety and other precautions survivors and organizations can employ.
http://www.vaw.umn.edu/documents/5survivortech/5survivortech.html

How Tracking Systems Place Victims at Risk: Homeless Management Information Systems &Victims of Abuse and Stalking
Author: Safety Net, NNEDV (2004)
Description: This handout discusses victim privacy concerns related to the collection, sharing, and storage of data, to ensure intimate partner stalkers cannot access data. It provides advocacy strategies to consider when community members want an organization to share identifiable victim data. The document focuses on the implementation of homeless databases in the U.S., but highlights safety concerns relevant to all victims of stalking and abuse.
http://www.nnedvfund.org/pdf/NNEDV_HMISTrackingVictims.pdf

Protect Your Phone Privacy /Proteja su Privacidad Telefonica
Author: Pennsylvania Coalition Against Domestic Violence (1998, in English and Spanish)
Description: This handout for victims of domestic violence, harassment, and stalking notes U.S. options for blocking telephone calls using "caller ID", "line blocking", and "per call blocking".
http://www.vawnet.org/PCADVPublications/Brochures/CallBlok.pdf

Public &Internet Access to Court Records: Safety &Privacy Risks for Victims of Domestic Violence &All Citizens Using the Justice System
Author: Safety Net, NNEDV (2003)
Description: This document provides information

viables pour garantir la confidentialité des renseignements personnels des victimes, qu'elles exercent leur droit de vote, achètent une propriété, comparaissent devant un tribunal ou s'adonnent à d'autres activités.

Annexe B : Liste annotée de ressources à l'intention des groupes de défense

La liste ci-dessous, à l'intention des groupes de défense travaillant auprès des survivantes de traque exercée par des moyens technologiques, met en relief une sélection de projets d'assistance technique, de sites Internet et de documents choisis pour leur utilité pratique.

A. Projets d'assistance technique aux États-Unis

Le Safety Net Project du National Network to End Domestic Violence Fund
660 Pennsylvania Ave SE, Suite 303; Washington, D.C. 20003
Téléphone : 202-543-5566, poste 22
Télécopieur : 202-543-5626
Courriel : safetynet@nnedv.org
http://www.nnedvfund.org
Description : Lancé en août 2002, Safety Net: the National Safe & Strategic Technology Project du National Network to End Domestic Violence Fund (NNEDV) traite de toutes les formes de technologies qui profitent aux survivantes, sont utilisées à mauvais escient par les agresseurs ou touchent les survivantes au sein de leurs communautés. Le Safety Net Project offre aux coalitions de lutte contre la violence familiale, aux intervenants locaux, aux représentants des forces de l'ordre, aux procureurs et à d'autres alliés à l'échelle des États américains, de la formation et de l'assistance technique sur toutes les formes de technologies qui ont une incidence sur la vie des victimes d'abus.

Le Stalking Resource Center du National Center for Victims of Crime
2000 M Street NW, Suite 480, Washington, D.C. 20036
TTY : 1-800-211-7996
Téléphone : 1-800-FYI-CALL (1-800-394-2255)
Télécopieur : 202-467-8701
http://www.ncvc.org/src
Description : Le Stalking Resource Center est un programme qui relève du National Center for Victims of Crime. Lancé en juillet 2000 grâce à regarding technology-stalking risks for victims and the importance of protecting victim privacy when court systems post partial or complete court records on the World Wide Web.

Stalking
Author: National Center for Victims of Crime (In Problem-Oriented Guides for Police Problem-Specific Guides Series No. 22, 2004)
Description: This guide covers the prevalence and nature of stalking, the impact of stalking on victims, and recognizes stalking as a pervasive tactic of those who perpetrate domestic violence. It mentions ways technology is used to stalk including: harassing telephone calls or emails, invasive computer monitoring programs, wiretapping, use of location devices and wireless remote cameras, and identity theft. The guide notes challenges to policing stalking and recommends responses to stalking, including practical suggestions for police around investigation.
http://www.cops.usdoj.gov/mime/open.pdf?item=1042

A Study on Cyberstalking: Understanding Investigative Hurdles
Author: Robert D'Ovidio &James Doyle (In FBI Law Enforcement Bulletin, March 2003, 10-17)
Description: This article summarizes the technological methods used by stalkers from cases reported to and investigated by New York City Police Department's Computer Investigation &Technology Unit from 1996 to 2000. Intimate partner stalking is not specifically addressed, however barriers to law enforcement holding cyberstalkers accountable including jurisdictional laws, internet service provider policies, and anonymizing tools are covered.
http://www.fbi.gov/publications/leb/2003/mar03leb.pdf

Technology Safety Planning with Survivors: Tips to Discuss if Someone You Know is in Danger /Un Plan de Protecci n de la Tecnolog a para las(os) Sobrevivientes
Author: Safety Net, NNEDV (2003, 2004 revised, in English and Spanish)
Description: This tip sheet provides technology related safety planning strategies for survivors, including telephones, GPS, computers, and the Internet.

Tips for Survivors of High-Tech Abuse and

des fonds de l'Office on Violence Against Women, le programme est investi d'une mission double, à savoir sensibiliser davantage la population à l'échelle du pays au sujet de la traque et favoriser l'élaboration et la mise en œuvre de mesures multidisciplinaires de lutte contre la traque dans les diverses communautés du pays. Le Stalking Resource Center offre de la formation et de l'assistance technique se rapportant à toutes les formes de traque (y compris à l'aide de la haute technologie) et à l'intervention communautaire. Il tient à jour un site Internet renfermant des articles, des reportages, des lois et des textes de jurisprudence sur la traque, ainsi que de nombreuses autres ressources à l'intention des groupes de défense et des victimes. De plus, il publie deux bulletins par année, de même que des brochures téléchargeables à partir de son site.

La National Domestic Violence Hotline/Linea Nacional sobre la Violencia Domestica
PO Box 161810, Austin, TX 78716
TTY : 1-800-787-3224
Téléphone : 1-800-799-SAFE (7233)
http://www.ndvh.org
Description : Cet info service sans frais permet aux victimes de violence familiale, à leurs familles, aux groupes de défense et aux amis de parler à des intervenants/conseillers qui leur fourniront, de manière confidentielle, une aide en cas de crise, un soutien, de l'information et des services d'aiguillage vers des programmes locaux. L'info service met en rapport les victimes avec les refuges et avec les programmes d'aide juridique et sociale de leur région. Les intervenants offrent leurs services en anglais et en espagnol, et font appel à des interprètes pour les étendre à 139 autres langues. L'aide en cas de crise et les services d'aiguillage sont accessibles aux malentendants grâce à une ligne TTY ou par courriel à l'adresse deafhelp@ndvh.org. L'info service est accessible 24 heures sur 24 n'importe où aux États-Unis.

B. Sites Internet sur les réponses à l'utilisation de la technologie aux fins de traque d'un partenaire intime

Privacy Rights Clearinghouse
http://www.privacyrights.org
Description : Privacy Rights Clearinghouse (PRC) est un programme à but non lucratif qui se consacre à l'éducation des consommateurs, à la recherche et à la défense des intérêts. Bien que

Stalking/Consejos para las(os) Sobrevivientes del Abuso y del Acoso de la Alta-Tecnolog a
Author: Safety Net, NNEDV (2003, in English and Spanish)
Description: This handout is designed for survivors and focuses on planning for safety, as well as collecting evidence in complex stalking via technology situations. The document reinforces the key role that a victim plays in identifying methods of technology stalking, provides a sample stalking log, and other documentation examples for a victim of stalking via technology.

Web Wise Women: Part 1 - Minimizing information published about you on the World Wide Web /Mujeres Sabias en la Web. Parte 1 - Disminuyendo la informaci n que ha sido publicada en el World Wide Web
Author: Safety Net, NNEDV (2003, in English and Spanish)
Description: This document is designed for survivors of intimate partner stalking who are trying to prevent their private information from being published to the Internet. Information regarding online search engines, court and government websites, private websites, and information brokers/sellers is covered.

Website Safety Alerts: Tips for Advocacy Organizations
Author: Safety Net, NNEDV (2002)
Description: This document summarizes changes victim advocacy organizations can make to their websites to better educate victims/ survivors about computer and Internet monitoring.

Appendix C: A Handout For Survivors

- Technology Safety Planning with Survivors

While Appendix A and B are intended to accompany this paper, Appendix C (following) can be distributed separately from the attached paper. Feel free to share the following technology safety plans with victims, advocates, and allies.

Technology Safety Planning with Survivors

Tips to discuss if someone you know is in danger. Technology can be very helpful to victims of domestic violence, sexual violence, and stalking, however it is important to also consider how technology might be misused.

1. **Trust your instincts.** If you suspect the

l'information diffusée par PRC s'adresse au grand public et ne porte pas uniquement sur la traque d'un partenaire intime, les groupes de défense trouveront sur le site de nombreuses fiches de renseignements, des discours et des articles comportant des survols et des conseils pratiques d'intérêt pour les survivantes, notamment sur la protection des renseignements personnels sur Internet, divers enjeux liés à l'utilisation du téléphone et aux télécommunications, et les dossiers publics et gouvernementaux.

Stalking Resource Center – Recueils de lois et d'affaires judiciaires se rapportant à la traque
Lois réprimant la traque : http://www.ncvc.org/src/main.aspx?dbID=DB_All_Legislation188
Affaires judiciaires sur des cas de traque : http://www.ncvc.org/src/main.aspx?dbID=DB_All_Case_Law508
Description : Ces recueils en ligne présentent des lois et des résumés d'affaires judiciaires relevant de différentes instances aux États-Unis : fédérale, inter-étatique fédérale, États et tribale. Ils contiennent de l'information que les groupes de défense et les survivantes trouveront utile sur les lois que l'on peut invoquer pour tenir un agresseur responsable de l'utilisation de la technologie à des fins de traque. La section des lois réprimant la traque propre à chaque État reproduit les textes de loi et les infractions connexes comme la traque par téléphone, la traque électronique et les communications informatiques illicites. La section des affaires judiciaires se rapportant à la traque résume les conclusions des affaires entendues par la cour fédérale et les tribunaux d'État, y compris les circonstances dans lesquelles l'utilisation de la technologie pour traquer un partenaire intime a été considérée comme étant un acte criminel.

SafetyEd International
http://www.safetyed.org
Description : Hébergé en Nouvelle-Zélande, ce site Web donne de l'information sur la sécurité et la protection des renseignements personnels en ligne. Il comprend des articles de recherche, des ateliers en ligne, des résumés d'affaires judiciaires aux États-Unis et d'autres articles de sensibilisation sur la traque électronique.

Working to Halt Online Abuse (WHOA)
http://www.haltabuse.org
Description : L'organisme WHOA lutte contre le harcèlement en ligne par la sensibilisation du grand public, l'éducation des représentants des

abusive person knows too much, it is possible that your phone, computer, email, or other activities are being monitored. Abusers and stalkers can act in incredibly persistent and creative ways to maintain power and control.

2. **Plan for safety.** Navigating violence, abuse, and stalking is very difficult and dangerous. Advocates at the National Domestic Violence Hotline have been trained on technology issues, and can discuss options and help you in your safety planning. Local hotline advocates can also help you plan for safety. (National DV Hotline: 1-800-799-7233 or TTY 800-787-3224)

3. **Take precautions if you have a "techy" abuser.** If computers and technology are a profession or a hobby for the abuser/stalker, trust your instincts. If you think he/she may be monitoring or tracking you, talk to a hotline advocate or the police.

4. **Use a safer computer.** If anyone abusive has access to your computer, he/she might be monitoring your computer activities. Try to use a safer computer when you look for help, a new place to live, etc. It may be safest to use a computer at a public library, community center, or Internet cafe.

5. **Create a new email account.** If you suspect that anyone abusive can access your email, consider creating an additional email account on a safer computer. Do not create or check this new email from a computer your abuser could access, in case it is monitored. Use an anonymous name, and account: (example: bluecat@email.com, not YourRealName@email.com) Look for free web-based email accounts, and do not provide detailed information about yourself.

6. **Check your cell phone settings.** If you are using a cell phone provided by the abusive person, consider turning it off when not in use. Also many phones let you to "lock" the keys so a phone won't automatically answer or call if it is bumped. When on, check the phone settings; if your phone has an optional location service, you may want to switch the location feature off/on via phone settings or by turning your phone on and off.

7. **Change passwords &pin numbers.** Some

forces de l'ordre et l'habilitation des victimes. Son site Web renferme des liens vers diverses ressources sur le harcèlement en ligne et la traque, et propose quelques conseils pour accroître la sécurité. WHOA se penche sur différents problèmes auxquels font face les victimes de traque par un étranger ou une connaissance, et bon nombre d'entre eux s'appliquent aussi à la traque d'un partenaire intime.

C. Écrits qui traitent des réactions à l'utilisation de la technologie pour traquer un partenaire intime

Address Confidentiality Programs
Auteur : Vote Power Project, NNEDV Fund (2004)
Description : Ce document donne la liste des États américains ayant des programmes de traitement confidentiel des adresses et fournit des numéros de téléphone et un accès Internet aux formulaires pertinents de ces États, de l'information sur l'admissibilité et une explication sur la marche à suivre.
http://www.nnedvfund.org/default.asp?Page=63

Annotated Stalking Bibliography
Auteur : Stalking Resource Center, National Center for Victims of Crime (NCVC)
Description : Cette bibliographie présente de brefs résumés de plus de trente documents sur la traque, tous publiés après 1994. Des notes indiquent si l'article traite de la traque ou du harcèlement électronique effectué par un partenaire intime.
http://www.ncvc.org/src/main.aspx?dbID=DB_Annotated_Stalking_Bibliography344

Data Security Checklist to Increase Victim Safety & Privacy
Auteur : Safety Net: the National Safe & Strategic Technology Project, the National Network to End Domestic Violence Fund (Safety Net, NNEDV) (2004)
Description : Cette liste indique les étapes à considérer lorsqu'on entreprend des activités comme la conception d'un système de collecte de données ou la sécurisation du réseau d'un organisme local. Ces conseils aident à préserver la confidentialité des données sur les victimes et à mieux les protéger des traqueurs utilisateurs de haute technologie et des pirates informatiques.
http://www.nnedvfund.org/pdf/NNEDVDataSecurity.pdf

abusers use victim's email and other accounts to impersonate and cause harm. If anyone abusive knows or could guess your passwords, change them quickly and frequently. Think about any password protected accounts - online banking, voicemail, etc.

8. **Minimize use of cordless phones or baby monitors.** If you don't want others to overhear your conversations, turn baby monitors off when not in use and use a traditional corded phone for sensitive conversations.

9. **Use a donated or new cell phone.** When making or receiving private calls or arranging escape plans, try not to use a shared or family cell phone because cell phone billing records and phone logs might reveal your plans to an abuser. Contact your local hotline program to learn about donation programs that provide new cell phones and/or prepaid phone cards to victims of abuse and stalking.

10. **Ask about your records and data.** Many court systems and government agencies are publishing records to the Internet. Ask agencies how they protect or publish your records and request that court, government, post office and others seal or restrict access to your files to protect your safety.

11. **Get a private mailbox and don't give out your real address.** When asked by businesses, doctors, and others for your address, have a private mailbox address or a safer address to give them. Try to keep your true residential address out of national databases.

12. **Search for your name on the Internet.** Major search engines such as "Google" or "Yahoo" may have links to your contact information. Search for your name in quotation marks: "Full Name". Check phone directory pages because unlisted numbers might be listed if you have given the number to anyone.

The copyright of this particular part of the article belongs to The NNEDV Fund 2003. Created 6/03, Revised 5/04 by Cindy Southworth, Shawndell Dawson, and Cynthia Fraser with Safety Net: the National Safe &Strategic Technology Project at the National Network to End Domestic Violence www.nnedv.org

Domestic Violence Organizations Online: Risks, Ethical Dilemmas, and Liability Issues
Auteur : Jerry Finn (2001)
Description : Cet article décrit quels sont les risques et les responsabilités liés à l'utilisation d'Internet pour les groupes de défense qui travaillent avec des survivantes de traque et de violence familiale. Il indique les risques que courent les survivantes en ce qui a trait à la protection de leur vie privée et à leur sécurité lorsqu'elles communiquent et accèdent à des services directs en ligne.
http://www.vaw.umn.edu/documents/commissioned/online_liability/online_liability.html

Helpful or Harmful? How Innovative Communication Technology Affects Survivors of Intimate Violence
Auteur : Ann L. Kranz (2001)
Description : Cet article explore de quelles façons les survivantes de violence intime et les organismes qui les servent utilisent le Web. Il montre comment les agresseurs utilisent la technologie des communications pour surveiller et contrôler les activités de leurs partenaires, et donne des informations sur les précautions et autres mesures de sécurité que les survivantes et les organismes peuvent prendre.
http://www.vaw.umn.edu/documents/5survivortech/5survivortech.html

How Tracking Systems Place Victims at Risk: Homeless Management Information Systems & Victims of Abuse and Stalking
Auteur : Safety Net, NNEDV (2004)
Description : Ce document examine les inquiétudes des victimes à l'égard de la protection de leurs renseignements personnels dans le contexte de la collecte, du partage et de l'entreposage des données, et leurs craintes que les traqueurs partenaires intimes aient accès à ces données. Il propose des stratégies de défense à examiner lorsque les membres d'une communauté demandent qu'un organisme partage des données qui permettent d'identifier une victime. Ce document vise la mise en œuvre de bases de données pour les sans-abri aux États-Unis, mais souligne les problèmes de sécurité que connaissent toutes les victimes de traque et d'agressions.
http://www.nnedvfund.org/pdf/NNEDV_HMISTrackingVictims.pdf

References

Associated Press. (1995, March 30). Man charged in caller ID killing. *Dallas Morning News,* p. A33.

Bahm, T. (2003, Summer). Eliminating "cyber-confusion". *Newsletter of the Stalking Resource Center, 3*(2) [Electronic Version]. Retrieved August 30, 2004, from the National Center for Victims of Crime website : http://www.ncvc.org/src/main.aspx?dbID=DB_Eliminating_Cyber-Confusion251

Brewster, M. (2003). Power and control dynamics in prestalking and stalking situations. *Journal of Family Violence, 18*(4), 207-217.

Cellular Telecommunications &Internet Association. (2004). *CTIA's semi-annual wireless industry survey, June 1985 - June 2004* [Electronic Version].Washington DC: Author. Retrieved February 20, 2005, from http://files.ctia.org/pdf/CTIAMidyear2004Survey.pdf

CyberAngels. (1999). Retrieved February 20, 2005, from http://www.cyberangels.org

Dean, K. (2000). The epidemic of cyberstalking. *Wired News.* Retrieved February 20, 2005, from http://www.wired.com/news/politics/0,1283,35728,00.html

Department of Justice. (1999). *1999 Report on cyberstalking: A new challenge for law enforcement and industry* [Electronic Version]. Washington, DC: U.S. Department of Justice, Office of the Attorney General. Retrieved July 7, 2004, from http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

Department of Justice. (2001). *Stalking and domestic violence: Report to Congress* (NCJ 186157).Washington, DC: U.S. Department of Justice.

Ellison, L., &Akdeniz, Y. (1998, December). Cyber-stalking: The regulation of harassment on the Internet. [Electronic Version]. *Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet,* 29-48. Retrieved February 20, 2005, from http://www.cyber-rights.org/documents/stalking_article.pdf
Finn, J. (2001). *Domestic violence organizations online: Risks, ethical dilemmas, and liability issues.* Retrieved July 7, 2004 from http://

Protect Your Phone Privacy/Proteja su Privacidad Telefónica
Auteur : Pennsylvania Coalition Against Domestic Violence (1998, en anglais et en espagnol)
Description : Ce document destiné aux victimes de violence familiale, de harcèlement et de traque présente les choix offerts aux États-Unis pour bloquer les appels téléphoniques en utilisant l'affichage des appels, le blocage de communications, et le blocage par appel.
http://www.vawnet.org/PCADVPublications/Brochures/CallBlok.pdf

Public & Internet Access to Court Records: Safety & Privacy Risks for Victims of Domestic Violence & All Citizens Using the Justice System
Auteur : Safety Net, NNEDV (2003)
Description : Ce document fournit des renseignements sur les risques que courent les victimes de traque technologique et sur l'importance de protéger leurs renseignements personnels lorsque les tribunaux affichent sur le Web des dossiers judiciaires partiels ou complets.

Stalking
Auteur : National Center for Victims of Crime (*In Problem-Oriented Guides for Police, Problem-Specific Guides,* n° 22, 2004)
Description : Ce manuel porte sur la fréquence et la nature de la traque et ses conséquences sur les victimes, et reconnaît que cette tactique envahissante est couramment employée par les auteurs de violence familiale. On y mentionne de quelle façon les technologies sont utilisées pour traquer les victimes : appels téléphoniques ou courriels malveillants, logiciels espions envahissants, branchements clandestins, utilisation d'appareils de localisation et de caméras sans fil télécommandées, et vol d'identité. Ce guide souligne les défis que doivent relever les services policiers pour lutter contre la traque et propose des réponses, dont des suggestions pratiques pour les enquêtes policières. http://www.cops.usdoj.gov/mime/open.pdf?item= 1042

A Study on Cyberstalking: Understanding Investigative Hurdles
Auteur : Robert D'Ovidio & James Doyle (*In FBI Law Enforcement Bulletin*, mars 2003, p. 10-17)
Description : Cet article résume les techniques utilisées par les traqueurs à partir de cas rapportés et ayant fait l'objet d'une enquête de l'unité des technologies et enquêtes informatiques

www.vaw.umn.edu/documents/commissioned/online_liability/online_liability.pdf

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence, 19*(4), 468-483.

Fisher, B. S., Cullen, F. T., &Turner, M. G. (2000). *The sexual victimization of college age women* (NCJ 182369).Washington, DC: U.S. Department of Justice, National Institute of Justice and Centers for Disease Control and Prevention.

Greenfeld, L. A., Rand, M. R., Craven, D., Klaus, P. A., Perkins, C. A., Ringel, C., et al. (1998). *Violence by intimates: Analysis of data on crimes by current or former spouses, boyfriends, and girlfriends* (NCJ 167237).Washington DC: U.S. Department of Justice.

H.E.S. v. J.C.S., 175 N.J. 309, 815 A.2d 405 (Sup. Ct. February 6, 2003). Retrieved February 20, 2005, from http://lawlibrary.rutgers.edu/decisions/supreme/a-132-01.opn.html

Jenson, B. (1996). *Cyberstalking: Crime, enforcement, and personal responsibility in the on-line world.* Retrieved May 30, 2004, from http://www.sgrm.com/art-8.htm

Kranz, A. L. (2001). *Survivors of intimate violence seek help online: Implications of responding to increasing requests.* Retrieved July 7, 2004, from http://www.vaw.umn.edu/documents/10vawpaper/10vawpaper.html

Lamberg, L. (2001). Stalking disrupts lives, leaves emotional scars. *Journal of American Medical Association, 286*(5), 519-523. Retrieved June 18, 2004, from http://jama.ama-assn.org/cgi/content/full/286/5/519

Laughren, J. (2000). *Cyberstalking awareness and education.* Retrieved May 30, 2004, from http://www.acs.ucalgary.ca/~darbent/380/webproj/jessica.html

Lee, R. (1998). Romantic and electronic stalking in a college context. *William and Mary Journal of Women and the Law, 4,* 373-466.

McFarlane, J. M., Campbell, J. C., Wilts, S., Sachs, C. J., Ulrich, Y., &Xu, X. (1999). Stalking and intimate partner femicide. *Homicide Studies, 3* (4), 300-316.

du New York City Police Department, de 1996 à 2000. Il ne traite pas précisément de la traque des partenaires intimes. Cependant, il couvre l'obstacle à l'application de la loi qu'est la difficulté de tenir les traqueurs électroniques responsables de leurs gestes, y compris les lois des États, les politiques des fournisseurs de services Internet et les outils pour préserver l'anonymat.
http://www.fbi.gov/publications/leb/2003/mar03leb.pdf

Technology Safety Planning with Survivors: Tips to Discuss if Someone You Know is in Danger/Un Plan de Protección de la Tecnología para las(os) Sobrevivientes
Auteur : Safety Net, NNEDV (2003, révisé en 2004, en anglais et en espagnol)
Description : Ce bulletin de conseils propose aux survivantes des stratégies de planification de la sécurité reliées à la technologie, y compris les téléphones, les GPS, les ordinateurs et Internet.

Tips for Survivors of High-Tech Abuse and Stalking/Consejos para las(os) Sobrevivientes del Abuso y del Acoso de la Alta-Tecnología
Auteur : Safety Net, NNEDV (2003, en anglais et en espagnol)
Description : Ce document est conçu pour les survivantes et traite principalement de la sécurité aussi bien que de la collecte de preuves dans des cas de traque technologique complexes. Ce document renforce le rôle essentiel des victimes dans l'identification des méthodes de ce type de traque et fournit un modèle de relevé d'épisodes de traque ainsi que d'autres exemples de documents destinés aux victimes de traque technologique.

Web Wise Women: Part 1 - Minimizing information published about you on the World Wide Web/Mujeres Sabias en la Web. Parte 1 - Disminuyendo la información que ha sido publicada en el World Wide Web
Auteur : Safety Net, NNEDV (2003, en anglais et en espagnol)
Description : Ce document est conçu pour les survivantes de traqueurs partenaires intimes qui essaient d'empêcher la publication de leurs renseignements personnels sur Internet. Il contient de l'information concernant les moteurs de recherche en ligne, les sites Web des cours de justice et du gouvernement, les sites Web privés, et les courtiers et marchands d'information.

Madden, M., &Rainie, L. (2003). *America's online pursuits: The changing picture of who's online and what they do.* Retrieved July 1, 2004, from http://www.pewinternet.org/pdfs/PIP_Online_Pursuits_Final.PDF

Maxwell, A. (2001). *Cyberstalking.* Retrieved May 30, 2004, from http://www.netsafe.org.nz/Doc_Library/cyberstalking.pdf

National Center for Victims of Crime. (2004). Stalking [Electronic Version]. *Problem-Oriented Guides for Police: Problem-Specific Guides Series No. 22.* Washington DC: U.S. Department of Justice, Office of Community Oriented Policing Services. Retrieved February 20, 2005, from http://www.cops.usdoj.gov/mime/open.pdf?item=1042

National Criminal Justice Association. (1993). *Project to develop a model anti-stalking code for states.* Washington, DC: U.S. Department of Justice, National Institute of Justice.

Ogilvie, E. (2000, September). Cyberstalking. *Trends &Issues in Crime and Criminal Justice,* 166 [Electronic Version]. Retrieve May 30, 2004, from http://www.aic.gov.au/publications/tandi/ti166.pdf

Orland, K. (2003, February 6). Stalker victims should check for GPS. *CBS News.com.* Retrieved July 7, 2004, from http://www.cbsnews.com/stories/2003/02/06/tech/main539596.shtml

Safety Net: The National Safe &Strategic Technology Project. (2004). *Safety net training curriculum: Technology, advocacy, and victim safety.* Washington, DC: The National Network to End Domestic Violence Fund.

Spitzberg, B., &Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media &Society, 4*(1), 71-92.

Stalking Resource Center. (2003, Summer). Stalking technology outpaces state laws. *Stalking Resource Center Newsletter, 3*(2), 1, 3-4 [Electronic Version]. Retrieved July 7, 2004, from http://www.ncvc.org/src/main.aspx?dbName=DocumentViewer&DocumentID33500
Tjaden, P., &Thoenes, N. (1998). *Stalking in America: Findings from the National Violence Against Women Survey* (NCJ

Website Safety Alerts: Tips for Advocacy Organizations
Auteur : Safety Net, NNEDV (2002)
Description : Ce document résume les changements que les organismes de défense des victimes peuvent apporter à leurs sites Web afin de mieux éduquer les victimes et les survivantes sur la surveillance de leur ordinateur et d'Internet.

Annexe C : Document pour les survivantes

- Planification de la sûreté des technologies avec les survivantes

Bien que les annexes A et B aient pour objet d'accompagner ce document, l'annexe C (suivante) peut être distribuée séparément. N'hésitez pas à partager les plans de sécurité technologique avec les victimes, les groupes de défense et leurs alliés.

Planification de la sûreté des technologies avec les survivantes

Conseils à proposer si une de vos connaissances est en danger.
La technologie peut être très utile aux victimes de violence familiale, de violence sexuelle et de traque. Cependant, il faut savoir qu'elle peut être aussi utilisée à mauvais escient.

1. **Fiez-vous à votre instinct.** Si vous pensez qu'un agresseur est trop bien renseigné sur votre compte, il se peut que votre téléphone, votre ordinateur, votre courrier électronique ou d'autres de vos activités soient surveillées. Les agresseurs et les traqueurs peuvent être incroyablement tenaces et trouver des moyens extrêmement créatifs de continuer à exercer leur puissance et le contrôle sur leurs victimes.

2. **Planifiez vote sécurité.** Il est très difficile et dangereux d'essayer d'échapper à des situations de violence, d'agression et de traque. Les intervenants de la ligne de secours National Domestic Violence Hotline ont reçu une formation sur les questions technologiques et peuvent discuter des choix à votre disposition et vous aider à planifier votre sécurité. Les intervenants des services locaux d'urgence peuvent aussi vous aider à planifier votre sécurité (National DV Hotline :

169592).Washington, DC: U.S. Department of Justice.

Webster, K. (2003, December 1). Victim advocates want names, addresses, records offline. *USA Today.* Retrieved February 20, 2005, from http://www.usatoday.com/tech/news/internetprivacy/2003-12-01-victim-privacy_x.htm

Wendland, M. (2001, September 6). State targets cyber spies: Belleville man accused of electronic voyeurism. *Detroit Free Press.* Retrieved July 8, 2004, from http://www.freep.com/money/tech/spy6_20010906.htm

Working to Halt Online Abuse (WHOA). (2003). *Online harassment statistics: Prior contact — 2000-2004.* Retrieved on June 28, 2004, from http://www.haltabuse.org/resources/stats/relation.shtml

1-800-799-7233 ou TTY 800-787-3224).

3. **Prenez des précautions si votre agresseur est versé en technologie.** Si votre traqueur/agresseur est informaticien ou fait de l'informatique son passe-temps, faites confiance à votre instinct. Si vous pensez qu'il vous surveille ou vous traque, parlez-en à un intervenant d'un service d'urgence ou à la police.

4. **Utilisez un ordinateur sans risque.** Si un agresseur peut accéder à votre ordinateur, il peut surveiller vos activités informatiques. Essayez d'utiliser un ordinateur sans risque quand vous recherchez de l'aide, un nouvel endroit où vivre, etc. Il est peut-être plus sûr d'utiliser l'ordinateur d'une bibliothèque publique, d'un centre communautaire ou d'un café Internet.

5. **Créez un nouveau compte de courrier électronique.** Si vous soupçonnez qu'un agresseur peut avoir accès à votre courrier électronique, pensez à créer un nouveau compte de courrier sur un ordinateur sûr. Ne créez pas ou ne consultez pas cette nouvelle adresse électronique à partir d'un ordinateur auquel votre agresseur pourrait avoir accès au cas où cet ordinateur serait surveillé. Choisissez un nom et un compte anonymes (p. ex., chatbleu@email.com et non pas Votrevrainom@email.com). Recherchez des comptes de courrier électronique gratuits, et ne donnez aucun renseignement personnel.

6. **Vérifiez les caractéristiques d'installation de votre cellulaire.** Si vous utilisez un cellulaire offert par l'agresseur, pensez à le fermer lorsque vous ne vous en servez pas. De nombreux cellulaires offrent aussi l'option de « bloquer » les touches afin que le téléphone ne réponde pas et ne lance pas un appel automatiquement s'il est heurté. Lorsque l'appareil est en fonction, vérifiez-en les caractéristiques. S'il est muni d'un service de localisation facultative, vous voudrez peut-être annuler cette fonction à partir des caractéristiques d'installation ou en fermant et en ouvrant l'appareil.

7. **Changez vos mots de passe et vos numéros d'identification personnels (NIP).** Certains agresseurs se servent du courrier électronique de leur victime et d'autres

comptes pour usurper leur identité et leur faire du tort. Si un agresseur connaît ou pourrait deviner vos mots de passe, changez-les vite et faites-le souvent. Pensez à tous vos comptes protégés par mots de passe : services bancaires électroniques, courrier vocal, etc.

8. **Utilisez le moins possible les téléphones sans fil et les moniteurs pour bébés.** Si vous ne voulez pas que d'autres personnes écoutent vos conversations, éteignez les moniteurs pour bébés lorsque vous ne les utilisez pas ou utilisez un téléphone à fil traditionnel pour les conversations délicates.

9. **Utilisez un téléphone cellulaire donné ou neuf.** Lorsque vous faites ou recevez un appel personnel ou préparez un plan de fuite, évitez d'utiliser un téléphone cellulaire que la famille partage parce que les dossiers de facturation et les relevés téléphoniques peuvent révéler vos plans à votre agresseur. Communiquez avec votre service d'urgence local pour vous renseigner sur les programmes de dons qui fournissent de nouveaux cellulaires ou des cartes de téléphone prépayées aux victimes d'agression et de traque.

10. **Renseignez-vous sur vos dossiers et vos données personnelles.** De nombreux tribunaux et organismes gouvernementaux publient des dossiers sur Internet. Demandez à ces organismes comment ils protègent ou publient vos dossiers et demandez que la cour, le gouvernement, le bureau de poste et d'autres entités scellent vos dossiers ou en restreignent l'accès pour protéger votre sécurité.

11. **Procurez-vous une boîte postale privée et ne donnez pas votre adresse réelle.** Lorsqu'une entreprise, un bureau de médecin et d'autres vous demandent votre adresse, ayez une adresse postale ou une adresse sûre à leur donner. Essayez d'empêcher que votre adresse résidentielle réelle figure dans les banques de données nationales.

12. **Recherchez votre nom sur Internet.** Les principaux moteurs de recherche comme Google ou Yahoo peuvent avoir des liens qui mènent à vos renseignements personnels. Effectuez une recherche sur votre nom entre

guillemets : "Nom complet". Vérifiez votre annuaire téléphonique parce qu'un numéro non inscrit peut quand même y figurer si vous l'avez donné à quelqu'un.

Les droits d'auteur de cette partie du document appartiennent au NNEDV Fund 2003. Cette partie a été créée le 6-03 et révisée le 5-04 par Cindy Southworth, Shawndell Dawson et Cynthia Fraser du Safety Net: the National Safe & Strategic Technology Project au National Network to End Domestic Violence, www.nnedv.org

Références

ASSOCIATED PRESS. « Man charged in caller ID killing », *Dallas Morning News* (30 mars 1995), p. A33.

BAHM, T. « Eliminating "cyber-confusion" », *Newsletter of the Stalking Resource Center, 3*(2) (été 2003) [version électronique]. Récupéré le 30 août 2004 sur le site Web du National Center for Victims of Crime : http://www.ncvc.org/src/main.aspx?dbID=DB_Eliminating_Cyber-Confusion251

BREWSTER, M. « Power and control dynamics in prestalking and stalking situations », *Journal of Family Violence, 18*(4) (2003), p. 207-217.

CELLULAR TELECOMMUNICATIONS & INTERNET ASSOCIATION. *CTIA's semi-annual wireless industry survey, June 1985 - June 2004* (2004) [version électronique] Washington D.C.: Author. Récupéré le 20 février 2005 sur le site http://files.ctia.org/pdf/CTIAMidyear2004Survey.pdf

CYBERANGELS. (1999). Récupéré le 20 février 2005 sur le site http://www.cyberangels.org

DEAN, K. « The epidemic of cyberstalking », *Wired News* (2000). Récupéré le 20 février 2005 sur le site http://www.wired.com/news/politics/0,1283,35728,00.html

DEPARTMENT OF JUSTICE. *1999 Report on cyberstalking: A new challenge for law enforcement and industry* [version électronique] (1999), Washington, D.C: U.S. Department of Justice, Office of the Attorney General. Récupéré le 7 juillet 2004 sur le site http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

DEPARTMENT OF JUSTICE. *Stalking and domestic violence: Report to Congress* (NCJ 186157) (2001) Washington, D.C.: U.S. Department of Justice.

ELLISON, L. et Y. AKDENIZ. « Cyber-stalking: The regulation of harassment on the Internet » (décembre 1998). [version électronique]. *Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet, p.* 29-48. Récupéré le 20 février 2005 sur le site : http://www.cyber-rights.org/documents/stalking_article.pdf

FINN, J. *Domestic violence organizations online: Risks, ethical dilemmas, and liability issues* (2001). Récupéré le 7 juillet 2004 sur le site http://www.vaw.umn.edu/documents/commissioned/online_liability/online_liability.pdf

FINN, J. « A survey of online harassment at a university campus », *Journal of Interpersonal Violence, 19*(4) (2004), p. 468-483.

FISHER, B. S., F.T. CULLEN ET M. G. TURNER. *The sexual victimization of college age women* (NCJ 182369) (2000).Washington, D.C.: U.S. Department of Justice, National Institute of Justice et Centers for Disease Control and Prevention.

GREENFELD, L. A., M. R. RAND, D. CRAVEN, P. A. KLAUS, C. A. PERKINS, C. RINGEL et al. *Violence by intimates: Analysis of data on crimes by current or former spouses, boyfriends, and girlfriends* (1998)(NCJ 167237). Washington D.C.: U.S. Department of Justice.

H.E.S. c. J.C.S., 175 N.J. 309, 815 A.2d 405 (Cour sup. le 6 février 2003). Récupéré le 20 février 2005 sur le site http://lawlibrary.rutgers.edu/decisions/supreme/a-132-01.opn.html

JENSON, B. *Cyberstalking: Crime, enforcement, and personal responsibility in the on-line world* (1996). Récupéré le 30 mai 2004 sur le site http://www.sgrm.com/art-8.htm

KRANZ, A. L. *Survivors of intimate violence seek help online: Implications of responding to increasing requests* (2001). Récupéré le 7 juillet 2004 sur le site http://www.vaw.umn.edu/documents/10vawpaper/10vawpaper.html

LAMBERG, L. « Stalking disrupts lives, leaves

emotional scars », *Journal of American Medical Association, 286*(5) (2001), p. 519-523. Récupéré le 18 juin 2004 sur le site http://jama.ama-assn.org/cgi/content/full/286/5/519

LAUGHREN, J. *Cyberstalking awareness and education* (2000). Récupéré le 30 mai 2004 sur le site http://www.acs.ucalgary.ca/~darbent/380/webproj/jessica.html

LEE, R. « Romantic and electronic stalking in a college context », *William and Mary Journal of Women and the Law, 4* (1998), p. 373-466.

MCFARLANE, J. M., J. C. CAMPBELL, S. WILTS, C. J. SACHS, Y. ULRICH ET X. XU. « Stalking and intimate partner femicide », *Homicide Studies, 3* (4), (1999), p. 300-316.

MADDEN, M. et L. RAINIE. *America's online pursuits: The changing picture of who's online and what they do* (2003). Récupéré le 1er juillet 2004 sur le site http://www.pewinternet.org/pdfs/PIP_Online_Pursuits_Final.PDF

MAXWELL, A. *Cyberstalking* (2001). Récupéré le 30 mai 2004 sur le site http://www.netsafe.org.nz/Doc_Library/cyberstalking.pdf

NATIONAL CENTER FOR VICTIMS OF CRIME. « Stalking » [version électronique], *Problem-Oriented Guides for Police: Problem-Specific Guides Series No. 22.* Washington D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services (2004). Récupéré le 20 février 2005 sur le site http://www.cops.usdoj.gov/mime/open.pdf?item=1042

NATIONAL CRIMINAL JUSTICE ASSOCIATION. *Project to develop a model anti-stalking code for states.* Washington, D.C.: U.S. Department of Justice, National Institute of Justice (1993).

OGILVIE, E. « Cyberstalking », *Trends & Issues in Crime and Criminal Justice,* 166 [version électronique] (septembre 2000). Récupéré le 30 mai 2004 sur le site http://www.aic.gov.au/publications/tandi/ti166.pdf

ORLAND, K. « Stalker victims should check for GPS », *CBS News.com* (6 février 2003). Récupéré le 7 juillet 2004 sur le site http://www.cbsnews.com/stories/2003/02/06/tech/main539596.shtml

SAFETY NET: THE NATIONAL SAFE & STRATEGIC TECHNOLOGY PROJECT. *Safety net training curriculum: Technology, advocacy, and victim safety.* Washington, D.C.: The National Network to End Domestic Violence Fund (2004).

SPITZBERG, B. et G. HOOBLER. « Cyberstalking and the technologies of interpersonal terrorism », *New Media & Society, 4*(1) (2002), p. 71-92.

STALKING RESOURCE CENTER. « Stalking technology outpaces state laws », *Stalking Resource Center Newsletter, 3*(2), 1, 3-4 [version électronique] (été 2003). Récupéré le 7 juillet 2004 sur le site http://www.ncvc.org/src/main.aspx?dbName=DocumentViewer&DocumentID33500

TJADEN, P. et N. THOENES. *Stalking in America: Findings from the National Violence Against Women Survey* (NCJ 169592). Washington, D.C.: U.S. Department of Justice (1998).

WEBSTER, K. « Victim advocates want names, addresses, records offline », *USA Today* (1er décembre 2003). Récupéré le 20 février 2005 sur le site http://www.usatoday.com/tech/news/internetprivacy/2003-12-01-victim-privacy_x.htm

WENDLAND, M. « State targets cyber spies: Belleville man accused of electronic voyeurism », *Detroit Free Press* (6 septembre 2001). Récupéré le 8 juillet 2004 sur le site http://www.freep.com/money/tech/spy6_20010906.htm

WORKING TO HALT ONLINE ABUSE (WHOA). *Online harassment statistics: Prior contact - 2000-2004* (2003). Récupéré le 28 juin 2004 sur le site http://www.haltabuse.org/resources/stats/relation.shtml



LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Liste de vérification de sécurité de données pour augmenter la protection et la vie privée

Date Security Checklist to Increase Victim Safety & Privacy

Safety Net



Dans cette ère électronique, nous avons tous besoin d'augmenter notre protection à la vie privée en termes de données. Cependant, les victimes d'harcèlement, de violence familiale et sexuelle ont des préoccupations plus grandes en besoin de sécurité et de protection. Toute entreprise de collecte de données, à l'intérieur d'une organisation locale ou entre certains fournisseurs de services, doit être prudemment planifiée, implantée et évaluée régulièrement car la protection et la vie privée des survivantes de violence en dépendent.

La sécurité des données comprend plusieurs problématiques allant d'empêcher l'accès non autorisé jusqu'à réduire les renseignements recueillis et partagés. Étant donné la complexité des risques à la protection dans ce travail, les bases de données devront être emmagasinées sur des serveurs séparés et à haute sécurité à l'intérieur et entre les différents utilisateurs et les fournisseurs de services afin de maintenir le privilège d'accès et la confidentialité.

Protection sur l'Internet : Le Projet de sécurité sur l'Internet donne de la formation pertinente pour l'intérêt des victimes et leurs conseillères. Consultez notre site Web www.nnedv.org/Safety/Net pour en savoir davantage.

AVIS IMPORTANT : Cette liste de vérification se veut d'abord de donner un point de départ de discussion sur la protection de la cliente et la sécurité des données aux organisations locales. Cependant, elle n'est pas destinée à remplacer une formation intensive. Veuillez contacter vos associations provinciales/territoriales en violence familiale et sexuelle pour discuter de collecte de données et des questions de sécurité ayant un impact sur les victimes dans votre communauté.

Avant de commencer à prendre des mesures en collecte de données

□ **Réduisez les données recueillies**
Réduisez ce qui est recueilli pour diminuer les risques de sécurité aux victimes et la responsabilité de votre organisation. Révisez les buts de votre organisation/projet et évaluez le processus de votre collecte de données. Sont-elles des alternatives moins exigeantes pour mesurer les résultats et rationaliser l'admission? Comment les données que vous

In this electronic age, we all have heightened data privacy needs. However, victims of stalking, domestic and sexual violence have even greater security and safety concerns. Any data collection initiative within a local organization or between several service providers must be carefully planned, implemented, and evaluated regularly -- the safety and privacy of violence survivors depends on it.

Data security includes a range of issues -- from preventing unauthorized access to minimizing information collected and shared. Given the complex safety risks in this work, databases may need to be stored on separate servers with tight security within and between different users and service providers, to maintain privilege and confidentiality.

IMPORTANT NOTE: This checklist is meant to give local organizations a starting point in discussing client safety and data security; it is not intended to replace intensive training. Please contact your domestic violence and sexual assault provincial/territory associations to discuss data collection & security issues impacting victims in your community. Safety Net: Safe & Strategic Technology Project also provides training on technology's impact on victims and their advocates.

Before you Begin your Data Collection Initiative

□ **Minimize Data Collected**
Minimize what is collected to lessen the safety risks to victims and your organization's liability. Review the goals of your organization/project and evaluate your data collection process. Are there less invasive alternatives to measure outcomes and streamline intake? How could the data you plan to collect be misused if accessed through legitimate or illegitimate means?

□ **Develop and Implement Clear Policies**
Develop clear policies and procedures that outline privacy practices for handling sensitive victim data. Communicate these policies regularly at orientation and meetings. Data security policies should address:

- The content of the record, how long it will exist, and who may have access to it
- Processes for survivors to opt-out, inspect, withdraw, or correct their data/records
- Collection, modification, use, and disclosure procedures for client identifiable data

planifiez recueillir peuvent être mal utilisées si elles sont accédées par des moyens légitimes et illégitimes.

□ **Développez et implantez des politiques claires**
Développez des politiques et des procédures claires qui mettent en évidence les pratiques à la vie privée en manipulant des données sensibles de la victime. Veuillez communiquer de ces politiques régulièrement aux sessions d'orientation et réunions. La sécurité des données doit aborder :

- Le contenu du dossier, la durée qu'il va exister et qui peut en avoir accès
- Les processus pour que les victimes puissent abandonner, inspecter, retirer ou corriger des données/dossiers
- Collecte, modification, utilisation et procédures de révélation pour les données identifiables de la cliente
- Processus pour les dossiers papiers et pour l'élimination des ordinateurs et d'autres contenus multimédia, en toute sécurité, qui pourraient contenir des données identifiables de la cliente
- Sélection, formation et processus de vérification des antécédents des individus qui ont accès à de l'information d'identification sensible et personnelle
- Processus pour protéger contre l'utilisation ainsi que l'accès non autorisés

□ **Menez des évaluations de facteurs relatifs à la vie privée**
Les agences gouvernementales ont commencé à mener des évaluations de facteurs relatifs à la vie privée (ÉFVP) qui abordent les types de renseignements recueillies, les buts de la collecte, les utilisations requises des renseignements, l'échange de renseignements, les notifications de la cliente et la sécurité de l'information. Le *U.S. Center for Democracy and Technology* offre des outils éducatifs pour des renseignements supplémentaires. Visitez leur site Web www.cdt.org/egov/handbook/privacy/shtml

□ Conservez les données séparées
Les bases de données ayant des renseignements et de l'information sensible doivent être protégées avec prudence. Il est important de conserver les dossiers électroniques de la conseillère séparés des

- Procedures for paper records and for the secure disposal of computers or other electronic media that contain client identified data
- Screening, training, and background check processes of individuals who have access to sensitive personally identifying information
- Procedures to protect against unauthorized use and unauthorized access

□ **Conduct Privacy Impact Assessments**
Government agencies are beginning to conduct Privacy Impact Assessments (PIA) to address: types of information collected, purposes for collection, the intended uses of information, information sharing, client notification, and information security. The U.S. Center for Democracy and Technology offers educational tools for additional information. Please see their website: www.cdt.org/egov/handbook/privacy.shtml

□ **Keep data Separate**
Databases with casenotes and other sensitive information must be carefully protected. It's important to keep a victim advocate's confidential electronic records separate from prosecution databases since defense attorneys may have the right to see prosecutor notes and may attempt to argue that various entities have access to each other's data if the databases are combined or even on the same server. Work with attorneys who specialize in confidentiality and privilege in addition to technology experts. Important Note: If data is shared it should be minimal and should not invade a victim's privacy.

□ **Limit Access Levels**
Limit the number of users who are authorized to view the most sensitive information. When determining access levels, your organization must consider safety risks if the data will be shared internally within one organization or across many organizations. It is critical to review local, provincial/territory, and federal laws that stipulate who can or can't access victim data, and under what circumstances.

bases de données des poursuites puisque les avocats à la défense peuvent avoir le droit de visualiser les notes du demandeur et peuvent tenter d'argumenter que des entités variées ont accès aux données si celles-ci sont combinées ou sur le même serveur. Travaillez avec des avocats qui sont spécialisés dans la confidentialité et le privilège tout en étant des experts en technologie. Avis important : Si les données sont échangées, ceci devrait être fait minimalement et ne devrait pas envahir la vie privée de la victime.

- **Limitez les niveaux d'accès**
  Limitez le nombre d'utilisateurs qui sont autorisés à visualiser l'information la plus sensible. Lorsque vous déterminez les niveaux d'accès, votre organisation doit considérer les risques à la sécurité si les données sont échangées à l'interne, à l'intérieur d'une organisation ou entre plusieurs organisations. Il est essentiel de réviser les lois locales, provinciales/territoriales et fédérales qui stipulent ceux qui peuvent ou ceux qui ne peuvent pas accéder aux données de la victime et dans quelles circonstances.

Les éléments critiques à inclure lorsque vous concevez votre système de données

- **Vérifiez pour votre sécurité**
  Embauchez un consultant de confiance et compétent ou une entreprise de sécurité pour vérifier la sécurité de votre réseau et du processus de données protégées. Les banques et les organisations de défense sont censées prendre tous les moyens nécessaires pour protéger leurs données; les pourvoyeurs de services aux victimes doivent protégés la vie des victimes (et leurs données) et ce, au même niveau. Une vérification de sécurité extérieure peut fournir une analyse en profondeur des mesures de protection qui sont faibles ou manquantes.

- **Conservez les données de la victime loin de l'Internet**
  La manière la plus sécuritaire de protéger l'information sensible de la cliente est d'utiliser des dossiers papiers ou avoir des ordinateurs séparés : un pour Internet/courriel et l'autre pour les données sensibles. Ces ordinateurs séparés ne devraient pas être sur le même réseau. Des logiciels garde-barrière et antivirus

Critical Elements to Include when Designing your Data System

- **Test Your Security**
  Hire a trusted and skilled consultant or security firm to test the security of your network and data protection procedures. Banks and defense organizations are expected to go to great lengths to protect their data; Victim Service Providers must protect the lives of victims (and their data) to the same levels. An outside Security Audit can provide an indepth analysis of security protections that are weak or missing.

- **Keep victim data away from the Internet**
  The safest way to protect sensitive client information is to use paper records or to have separate computers: one for Internet/email and another for all sensitive data. These separate computers should not be networked together. Firewalls and anti-virus programs are helpful (see below), but can be compromised. When lives are on the line…keep data safe.

- **Utilize Anti-Virus Software & Firewalls**
  If you have an office network, consider the corporate addition of anti-virus, anti-spyware and firewall programs because the server automatically updates itself and each desktop connected to the server. Anti-Virus, anti-spyware protection and software or hardware Firewalls are important security steps for any organization with Internet access, however are not secure enough to adequately protect victim and client-identifiable data.

- **Use Alphanumeric Passwords and Change them Frequently**
  Password management is a critical part of data security. Alphanumeric passwords are a combination of upper and lower case letters, numbers and symbols. The use of pet names, birthdays, or words in a dictionary should be prohibited. Passwords should be changed frequently and kept safe; do not keep under the keyboard or taped to the monitor! A password-activated screen-saver for employees with access to sensitive information helps increase data security when they step away from their computers.

- **Use Encryption**
  Encryption is the conversion of data into a form that cannot be easily understood by unauthorized users. Encryption is not the solution to all security concerns; it is a small piece of a com-

sont utiles (voir ci-dessous) mais risquent d'être compromis. Lorsque des vies sont en jeu….conservez les données en sûreté.

- **<u>Utilisez des logiciels antivirus et garde-barrière</u>**
  Si vous avez un réseau au bureau, considérez l'addition corporative de logiciels antivirus, espions et garde-barrière car le serveur se met à jour automatiquement ainsi que les logiciels d'ordinateurs de bureau branchés au serveur. La protection antivirus, espion, ainsi que les logiciels garde-barrière, sont des mesures de sécurité importantes pour toute organisation ayant accès à l'Internet. Cependant, ces mesures ne sont pas assez sécuritaires pour protéger adéquatement la victime et les données identifiables de la cliente.

- **<u>Utilisez des mots de passe alphanumériques et changez-les souvent</u>**
  La gestion de mots de passe est un élément crucial de la sécurité de données. Les mots de passe alphanumériques sont une combinaison de lettres majuscules et minuscules, des chiffres et des symboles. L'utilisation de noms d'animaux de compagnie, d'anniversaires ou de mots dans le dictionnaire doit être défendue. Les mots de passe doivent être changés souvent et conservés en sûreté; ne pas les laisser en dessous du clavier ou collés au moniteur! Un économiseur d'écran avec activation du mot de passe pour les employés ayant accès à de l'information sensible aide à augmenter la sécurité des données lorsque les employés sont loin de leur ordinateur.

- **<u>Utilisez du chiffrement</u>**
  Le chiffrement est la conversion des données dans une forme qui ne peut être comprise facilement par des utilisateurs non autorisés. Le chiffrement n'est pas la solution à toutes les préoccupations reliées à la sécurité; il n'est qu'une petite partie de la solution compréhensible à la sécurité. Les institutions financières et les agences gouvernementales utilisent le chiffrement pour protéger les données entreposées et les données en transit vers leurs réseaux.

Maintien continu, vérification et formation

- **<u>Mettez à jour les systèmes d'exploitation</u>**
  Téléchargez régulièrement tous les derniers

prehensive security solution. Financial institutions and government agencies use encryption to protect stored data and data in transit over their networks.

Ongoing Maintenance, Audits, and Training

- **<u>Update Operating Systems</u>**
  Regularly download all the latest patches and updates for your operating systems. Sometimes the automatic Windows Update feature is not set up correctly, so it is important to check for updates weekly at the Microsoft website: www.microsoft.com

- **<u>Audit for Quality Assurance</u>**
  This is a process of evaluating data collected and removing any incorrect information. At minimum, staff responsible for the day-to-day data entry should not be in charge of the audit. Audits should include random samples of information collected about clients to help assess quality, accuracy, and to identify if inappropriate data is being collected or shared.

- **<u>Use Skilled Technology Professionals</u>**
  Most non-profit organizations do not have a full-time Information Technology Specialist, however, it is imperative that organizations collecting potentially lethal electronic data have qualified professional technical support. To limit cost, ask organizations that have been used as national models about their databases, their overall design, and the possibility of contracting to use their database as a starting point.

- **<u>Seek Ongoing Education</u>**
  Attend issue specific trainings or bring a consultant to your organization to speak about data security & victim safety. With high turnover, it is especially important to offer ongoing training & education to maintain the security of data and the safety of victims.

This checklist cannot cover every issue relevant to data security, but offers a list of key issues to consider.

correctifs et les mises à jour de vos systèmes d'exploitation. Quelquefois, la fonction automatique de Windows Update peut ne pas être installée correctement donc, il est important d'effectuer la mise à jour à chaque semaine sur le site Web Microsoft www.microsoft.com

- **Vérifiez pour une assurance de qualité**
  Ceci est un processus d'évaluation des données recueillies et de retrait de toute information incorrecte. Le personnel responsable de l'entrée quotidienne des données ne devrait pas être mandaté è faire cette vérification. La vérification devrait comprendre des prélèvements de contrôle de l'information recueillie sur les clients pour aider à évaluer la qualité, la fiabilité et à identifier si des données inappropriées ont été recueillies ou échangées.

- **Ayez recours aux professionnels en technologie**
  La plupart des organisations à but non lucratif n'ont pas de spécialiste en technologie à plein temps. Cependant, il est impératif que les organisations qui recueillent des données électroniques potentiellement à risque mortel aient recours à du support technique professionnel. Afin de limiter les frais, demandez aux organisations qui ont été utilisées comme des modèles à l'échelle nationale, à propos de leurs bases de données, leur design global et la possibilité de conclure un contrat pour utiliser leur base de données comme point de départ.

- **Recherchez l'éducation en cours**
  Participez à de la formation spécifique sur la problématique ou faites venir un consultant à votre organisation pour parler de la sécurité des données et de la protection de la victime. Les organisations ayant une forte rotation de personnel, il est spécialement important d'offrir de la formation et de l'éducation continue pour maintenir la sécurité des données et la protection des victimes.

Cette liste de vérification ne peut pas couvrir toutes les questions relevant de la sécurité des données mais offre une liste des problématiques essentielles à considérer.



LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Planification de la technologie de la sécurité avec les survivantes

Technology Safety Planning with Survivors

Safety Net

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Conseils pour discussion si une personne que vous connaissez est en danger

La technologie peut être utile aux victimes de violence familiale, violence sexuelle et d'harcèlement. Cependant, il est également important de considérer comment la technologie peut être mal utilisée.

1. Faites confiance à votre instinct. Si vous suspectez qu'une personne abusive en sait trop sur vous, il est possible que votre téléphone, ordinateur, courriel, vos sorties en voiture ou d'autres activités soient surveillés. Les abuseurs et les harceleurs peuvent être incroyablement persistants et utiliser toutes sortes de manières créatives pour maintenir leur pouvoir et le contrôle.

2. Planifiez votre sécurité. Naviguer sur la violence, l'abus et l'intimidation est très difficile et dangereux. En cas de violence familiale, de viol ou de crises, nous vous suggérons de contacter les lignes d'aide locales et provinciale/territoriales ainsi que les organisations pour discuter des options et des risques à la sécurité. Le projet de sécurité sur Internet peut supporter les agences en ce qui concerne l'harcèlement technologique ou les enjeux à la sécurité que vous subissez et qui sont nouveaux ou inconnus à leur personnel.

3. Prenez des précautions si vous avez un abuseur «techno». Si les ordinateurs et la technologie sont la profession ou le passe-temps de l'abuseur/harceleur, faites confiance à votre instinct. Si vous croyez que quelqu'un pourrait vous surveiller ou vous retracer, parlez-en aux intervenantes des lignes d'aide ou à la police.

4. Utilisez un ordinateur plus sécuritaire. Si une personne abusive a accès à votre ordinateur, elle pourrait surveiller vos activités sur l'ordinateur. Essayez d'utiliser un ordinateur plus sécuritaire lorsque vous recherchez de l'aide, un nouvel endroit pour habiter, etc. Il serait plus sécuritaire d'utiliser un ordinateur dans une bibliothèque, un centre communautaire ou un café Internet.

5. Créez un nouveau courriel ou CMI. Si vous suspectez qu'une personne abusive peut avoir accès à votre courriel ou vos comptes de messagerie instantanée (CMI), veuillez envisager de créer des courriels/CMI supplémentaires sur un ordinateur plus sécuritaire. Cependant, n'allez

Tips to discuss if someone you know is in danger

Technology can be very helpful to victims of domestic violence, sexual violence, and stalking, however it is important to also consider how technology might be misused.

1. Trust your instincts. If you suspect an abusive person knows too much, it is possible that your phone, computer, email, driving or other activities are being monitored. Abusers and stalkers can act in incredibly persistent and creative ways to maintain power and control.

2. Plan for safety. Navigating violence, abuse, and stalking is very difficult and dangerous. We suggest you contact local and provincial/territory domestic violence or rape crisis hotlines and organizations to discuss options and safety risks. The Safety Net Project can support agencies in any technology stalking or safety issues you experience that are new or unfamiliar to their staff.

3. Take precautions if you have a "techy" abuser. If computers and technology are a profession or hobby for the abuser/stalker, trust your instincts. If you think someone may be monitoring or tracking you, talk to hotline advocates or police.

4. Use a safer computer. If anyone abusive has access to your computer, he/she might be monitoring your computer activities. Try to use a safer computer when you look for help, a new place to live, etc. It may be safer to use a computer at a public library, community center, or Internet café.

5. Create new email or IM accounts. If you suspect that anyone abusive can access your email or instant messaging (IM), consider creating additional email/IM accounts on a safer computer. Do not create or check this new email/IM from a computer the abuser could access, in case it is monitored. Look for free web-based email accounts, and strongly consider using non-identifying name & account information. (example: bluecat@email.com and not YourRealName@email.com)

6. Check your cell phone settings. If you are using a cell phone provided by the abusive person, consider turning it off when not in use. Also, many phones let you to "lock" the keys so a phone won't automatically answer or call if bumped.

pas créer ou vérifier ces nouveaux courriels/CMI d'un ordinateur où votre abuseur pourrait avoir accès et pourrait vous surveiller. Utilisez plutôt des comptes de courriel gratuits sur l'Internet et envisagez d'utiliser des noms et des comptes non identifiables (par ex., chatbleu @courriel.com et non Votrenom@courriel.com)

6. Vérifiez vos options de cellulaire. Si vous utilisez un cellulaire fourni par la personne abusive, envisagez de le fermer lorsque non utilisé. Aussi, plusieurs téléphones vous permettent de «verrouiller» les touches ce qui empêchera à votre cellulaire de répondre ou d'ouvrir automatiquement lorsque l'appel est saisi. Vérifiez vos options de cellulaire lorsqu'il est ouvert; s'il a un service d'emplacement optionnel, vous voudrez peut-être changer la fonction d'emplacement à off ou on par les fonctions du cellulaire ou en ouvrant ou en fermant tout simplement votre téléphone.

7. Changez les mots de passe et les NIP. Certains abuseurs utilisent les courriels de leur victime et d'autres comptes pour les imiter et faire du tort. Si une personne abusive connaît ou pourrait deviner vos mots de passe, changez-les rapidement et souvent. Pensez à tous les comptes protégés par des mots de passe : banque en ligne, boîte vocale, messagerie électronique, etc.

8. Utilisez moins souvent les portables ou les moniteurs pour bébés. Si vous ne voulez pas que les autres entendent vos conversations, fermez les moniteurs de bébés si non utilisés et utilisez les téléphones traditionnels pour les conversations privées.

9. Utilisez un nouveau ou un cellulaire qui vous a été donné. Lorsque vous faites ou recevez des appels privés ou planifiez des arrangements pour fuir, essayez de ne pas utiliser un cellulaire partagé ou familial car les factures ou états de compte du cellulaire et le journal des appels pourraient révéler vos plans à l'abuseur. Contactez votre organisation et ligne d'aide locales et provinciale/territoriales pour connaître les programmes de dons qui fournissent des téléphones cellulaires neufs gratuitement et/ou des cartes d'appels prépayées aux victimes d'abus et d'harcèlement.

10. Demandez à propos de vos dossiers et de vos données. Quelques systèmes judiciaires,

When on, check the phone settings; if your phone has an optional location service, you may want to switch the location feature off/on via phone settings or by turning your phone on and off.

7. Change passwords & pin numbers. Some abusers use victim's email and other accounts to impersonate and cause harm. If anyone abusive knows or could guess your passwords, change them quickly and frequently. Think about any password protected accounts: online banking, voicemail, instant messaging, etc.

8. Minimize use of cordless phones or baby monitors. If you don't want others to overhear your conversations, turn off baby monitors if not needed and use traditional corded phones for sensitive conversations.

9. Use a donated or new cell phone. When making or receiving private calls or arranging escape plans, try not to use a shared or family cell phone because cell phone billing records and phone logs might reveal your plans to an abuser. Contact your local or provincial/territory hotline/ crisis organization to learn about donation programs that provide new free cell phones and/or prepaid phone cards to victims of abuse and stalking.

10. Ask about your records and data. Some court systems, government agencies and organizations publish records with personal information on the Internet. Ask agencies how they protect or publish your records and request that court, government, post office and others seal or restrict access to your files to protect your safety.

11. Get a private mailbox and don't give out your real address. When asked by businesses, doctors, and others for your address, have a private mailbox address or a safer address to provide. Try to keep your true residential address out of databases.

12. Search for your name on the Internet. Major search engines such as "Google" or "Yahoo" may have links to your contact information. Search for your name in quotation marks: "Full Name". Check phone directory pages because unlisted numbers might be listed if you gave your number to anyone.

agences gouvernementales et des organisations publient des dossiers sur l'Internet qui contiennent de l'information personnelle. Demandez leur comment ils protègent ou publient votre dossier et exigez que la cour, le gouvernement, le bureau de poste et autres organismes scellent ou restreignent l'accès à vos dossiers pour protéger votre sécurité.

11. Procurez-vous une boîte aux lettres privée et ne donnez pas votre adresse civique. Lorsque des entreprises, médecins ou d'autres personnes demandent votre adresse, ayez une adresse de boîte aux lettres privée ou une adresse plus sécuritaire à leur donner. Essayez de ne pas laisser votre adresse résidentielle civique dans des bases de données.

12. Cherchez pour votre nom sur l'Internet. Les moteurs de recherche importants tels «Google» ou «Yahoo» peuvent avoir des liens de contact à votre information. Cherchez pour votre nom entre guillemets «Nom au complet». Vérifiez les pages de l'annuaire téléphonique car des numéros confidentiels peuvent être listés si vous avez donné votre numéro à d'autres personnes.

Ontario Anonymous & Confidential 24X7 hotlines:
Assaulted Women's Helpline awhl.org

1-866-863-0511 or TTY 1-866-863-7868
FEMAIDE French-language hotline briserlesilence.ca
1-877-336-2433 (fem-aide) or ATS 1-866-860-7082

Search for Canadian shelters at **Shelternet.ca**
Canadian Association of Sexual Assault Centres **casac.ca**
Nat'l Aboriginal Circle Against Family Violence **nacafv.ca**
Email Safety Net Project at **SafetyNet@nnedv.org**

Lignes d'aide anonymes et confidentielles de l'Ontario 24 h /7 :

Assaulted Women's Helpline awhl.org
1-866-863-0511 ou TTY 1-866-863-7868

Ligne de soutien pour femmes victimes de violence briserlesilence.ca
1-877-336-2433 (fem-aide) ou ATS 1-866-860-7082

Lignes d'aide anonymes et confidentielles de Québec *24 h /7:*
S.O.S. violence conjugale ...De l'aide au bout du fil sosviolenceconjugale.com
1-800-363-9010

Recherche pour les maisons d'hébergement canadiennes: **Shelternet.ca**
Association canadienne des centres contre le viol : **casac.ca**
Le Cercle national autochtone contre la violence familiale : **nacafv.ca**
Courriel du Projet de sécurité sur l'Internet : **SafetyNet@nnedv.org**